UNIONE EUROPEA
REPUBBLICA ITALIANA
REGIONE SICILIANA
PRESIDENZA DELLA REGIONE SICILIANA
DIPARTIMENTO DELLA PROGRAMMAZIONE
AREA 3 AFFARI GENERALI – PERSONALE – BILANCIO – COMUNICAZIONE
TRASPARENZA – CONTRATTI

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL' ARCHIVIO DEL DIPARTIMENTO REGIONALE DELLA PROGRAMMAZIONE

1. Principi generali

1.1 PREMESSA

Il decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica del 20 ottobre 1998[1] n. 428", all'art. 3, comma 1, lettera c), prevede per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del Manuale di gestione.
Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio".
In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DsPR n. 428 del 20 ottobre 1998). Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.
Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.
Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.
Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.
Esso disciplina:

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

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

1.2 AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, recante le regole tecniche per il protocollo informatico.
Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Dipartimento Regionale della Programmazione.

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

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

1.3 DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:

- per "amministrazione", Dipartimento Regionale delle Programmazione;
- per "servizio informatico", Area 2 - Coordinamento monitoraggio programmi comunitari e nazionali;
- per "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per Regole tecniche, il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428;
- per Codice, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale.

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

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

Per le Norme ed i Regolamenti di riferimento vedasi l'elenco riportato nell'allegato 16.2.

1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

Per la gestione dei documenti, l'amministrazione ha adottato un modello organizzativo di tipo distribuito istituendo al suo interno la Area Organizzativa Omogenea (AOO) elencata nell'allegato 16.3.
All'interno della AOO il sistema di protocollazione è unico.
Nella AOO è istituito un servizio per la amministrazione del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Nel medesimo allegato, per la AOO è riportato: la denominazione, il codice identificativo della AOO, l'insieme degli UOR.
All'interno della AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in ingresso e in uscita; in questo caso ogni UOR svolge anche i compiti di UOP.

L'allegato 16.3 è suscettibile di modifica in caso di inserimento di nuove (AOO)UOP/UOR o di riorganizzazione delle medesime.
Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali.

1.5 SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

Nella AOO precedentemente individuata è istituito un servizio per la amministrazione del protocollo informatico, la gestione dei flussi documentali..
Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (Dirigente della Area 3 di seguito RSP).
Egli è funzionalmente individuato nell'Area 3 – Area Affari Generali alle dirette dipendenze della Direzione dell'Amministrazione, nominato con atto D.D.G. 01/A3 D.R.P. del 11 GEN 2017.

Al servizio è preposto un dirigente ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.
L'atto che istituisce il servizio e individua il responsabile della AOO è riportato nell'allegato 16.4, unitamente:

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

È compito del servizio:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale (eventualmente anche sul sito Internet dell'amministrazione);
- ove necessario proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- verificare il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare gli addetti dell'amministrazione all'utilizzo del PdP e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.);
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO;
- attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- verificare le funzionalità del sistema ed eventualmente contattare il gestore del servizio affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- verificare la corretta conservazione nelle copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- verificare il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

1.6 CONSERVAZIONE DELLE COPIE DI RISERVA

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, va riversato, nel rispetto della normativa vigente, su appositi sistemi di storage.
Tali supporti sono conservati da persona diversa da colui che ha realizzato il riversamento e dal RSP.
Le procedure di riversamento sono illustrate nel piano di sicurezza del MdG.

1.7 FIRMA DIGITALE

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.
Nell'allegato 16.5 viene riportato l'elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione.

1.8 TUTELA DEI DATI PERSONALI

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

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

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

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 3.
In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

1.9 CASELLE DI POSTA ELETTRONICA

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

1.10 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

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

1.11 FORMAZIONE

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

1.12 ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA

dipartimento.programmazione@certmail.regione.sicilia.it è la casella di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della Area 3; l'Area 3 procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.
L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico dal CNIPA fornendo le seguenti informazioni che individuano l'amministrazione stessa e la AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;
- l'indirizzo della sede principale della amministrazione;

Tali informazioni sono consultabile al link http://www.indicepa.gov.it/ricerca/n-dettaglioaoo.php?cod_amm=r_sicili&cod_aoo=RS003

1.13 PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dal DPCM 3 dicembre 2013. Giornalmente, attraverso una estrapolazione dal PdP, viene salvato il registro giornaliero di protocollo presso un ente certificato per la conservazione sostitutiva.

2. Eliminazione dei protocolli diversi dal protocollo informatico

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

2.1 PIANO DI ATTUAZIONE

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati.
Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di settore, di reparto e multipli. A tal fine sono state svolte le seguenti attività:

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

Le informazioni raccolte ed il piano di azione che ne è derivato, tengono conto della realtà organizzativa dell'AOO e della necessità di gestire la eventuale fase transitoria connessa con l'esaurimento delle pratiche in essere, protocollate e gestite anteriormente all'avvio del sistema di protocollo informatico e gestione documentale di cui al presente Manuale.
Il RSP esegue comunque, periodicamente, dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie UOP/UOR, 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 trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

3.2 GENERALITÀ

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

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

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- blocco della User id in caso di non utilizzo dello stesso per 6 mesi;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- ove possibile conservazione, a cura del servizio informatico, delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo.

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

3.3 FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA

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

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, preferibilmente in formato PDF o XML come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la

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

3.4 GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).
Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione degli accessi di ciascun utente autorizzato(amministratore di dominio), in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.4.1 COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.
L'Area deputata allo svolgimento delle attività informatiche è l'Area Coordinamento monitoraggio programmi comunitari e nazionali. Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- **Responsabile del sistema di sicurezza è il Dirigente Responsabile dell'Area 3 Affari Generali – Personale – Bilancio – Comunicazione – Trasparenza – Contratti**

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

- **Responsabile della sicurezza fisica è la società SiciliaDigitale che è responsabile degli accessi fisici alle stanze dei server e della sicurezza informatica del Protocollo**

3.4.2 COMPONENTE FISICA DELLA SICUREZZA

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

- **I server che gestiscono il protocollo ed i suoi allegati sono gestiti dalla società SiciliaDigitale che è responsabile degli accessi fisici alle stanze dei server e della sicurezza informatica del Protocollo.**

3.4.3 COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del PdP, è garantita attraverso l'utilizzo del Sistema Iride sviluppato dalla società CEDAf di Forlì secondo la normativa vigente in merito a sicurezza ed accessibilità ai dati; inoltre Tale applicativo viene aggiornato costantemente dalla società che lo detiene in modo da garantire il rispetto delle normative vigenti(Attualmente la versione in uso è la 1.4.A.45.537 aggiornata in data 07/12/2016).

3.4.4 COMPONENTE INFRASTRUTTURALE DELLA SICUREZZA

Nel server che ospita il sistema IRIDE è installato Windows server 2003 (costantemente aggiornato con la patch rilasciato da Microsoft) e si trova all'interno della infrastruttura di rete del Dipartimento Programmazione protetto da antivirus costantemente aggiornato.

3.4.5 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA

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

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

La sicurezza è garantita sia dal punto di vista del sistema operativo che registra, tramite log di sistema, tutti gli accessi sul sistema sia dal punto di vista dell'applicativo IRIDE che attraverso la scrittura su apposite tabelle conserva tutte le informazioni relative a modifiche di dati sui protocolli esistenti e, in generale, tutti i dati che possono essere utili per conoscere la storia di un protocollo dalla creazione in poi. Tali dati sono conservati all'interno del server dove risiede il protocollo e possono essere richiesta dal RSP alla società Sicilia Digitale.

3.5 TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.
Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata, ove richiesto, la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

3.5.1 ALL'ESTERNO DELLA AOO (INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.
Il sistema di protocollo informatico in uso al Dipartimento della Programmazione prevede, attraverso una corretta configurazione, la possibilità di ricevere direttamente documenti da protocollare attraverso una casella di posta elettronica certificata.

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 dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica (eventualmente certificata ai sensi del decreto del Presidente della Repubblica n. 68 dell'11 febbraio 2005) in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente "l'impiego della posta elettronica nelle pubbliche amministrazioni".
L'interscambio dei documenti si potrà svolgere anche attraverso l'utilizzo di aree di condivisione documentale appositamente predisposte dal servizio informatico, almeno una per ogni struttura intermedia dell'amministrazione.

3.6 ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono:

- la consultazione,
- l'inserimento,
- la modifica,
- l'annullamento.

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

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

Ogni utente autorizzato ad accedere al protocollo informatico Iride viene profilato in base alla propria Area/UOB/servizio di appartenenza ed in base al ruolo che in esso ricopre. In fase di creazione della utenza viene assegnata una password provvisoria che l'utente modifica al primo accesso. Ogni utente, che per 6 mesi consecutivi non accede al protocollo, viene bloccato e per essere riattivato deve chiedere l'intervento dell'amministratore di sistema.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

3.6.1 UTENTI INTERNI ALLA AOO

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

- Alcuni utenti autorizzati dal'RSP della Area 3 e dell'Area 1 del Dipartimento programmazione sono abilitati ad inserire documenti in ingresso.
- Tutti gli utenti del protocollo informatico sono abilitati alla consultazione di documenti interni alla loro struttura e all'inserimento di documenti in uscita.
- I responsabili delle Aree/UOB/servizi (o alle risorse da loro indicate) sono abilitati allo spostamento ed alla assegnazione dei documenti.
- L'amministratore del protocollo è autorizzato, previa richiesta scritta, alla modifica delle informazioni o alla cancellazione totale di un protocollo.

3.6.2 UTENTI ESTERNI ALLA AOO PRIVATI

L'esercizio del diritto di accesso ai documenti è possibile attraverso l'Ufficio Relazioni con il Pubblico (URP).
Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

3.7 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

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

3.7.1 SERVIZIO ARCHIVISTICO

Il responsabile del protocollo informatico dell'AOO (Dirigente della Area 3) ha individuato nei locali della società Sicilia Digitale la sede dell'archivio informatico dell'amministrazione.
Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza). Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.
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 responsabile del protocollo e anche responsabile della conservazione sostitutiva del registro giornaliero del protocollo e fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida, per una corretta esecuzione delle operazioni di salvataggio dei dati.
Il responsabile della conservazione digitale:

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

3.7.3 CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DELLE REGISTRAZIONI DI PROTOCOLLO

I luoghi di conservazione previsti per i supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza sono gestiti dalla società Sicilia Digitale che è responsabile della corretta conservazione e della gestione dei Backup.
In aggiunta viene fatto un export giornaliero del registro di protocollo che viene conservato presso un ente certificato per la conservazione sostitutiva dei documenti digitali(come previsto dal DPCM 3 DICEMBRE 2013).

È stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle eventuali diverse versioni) necessari alla lettura dei supporti conservati.
Il personale addetto alla sicurezza del sistema informatico 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

Tutti i file contenenti i backup di cui al paragrafo 3.7.3 sono conservati a cura della società Sicilia Digitale che è responsabile della loro conservazione e sicurezza.

3.8 POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.
È compito del RSP, assistito dal responsabile della sicurezza e/o del responsabile del sistema informativo e/o del responsabile della tutela dei dati personali, procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di audit.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

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

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.
Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo.
Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

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

Il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005:

1. *"Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71,*
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 ecc., consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

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

4.2 DOCUMENTO INVIATO

I documenti informatici, compresi di eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.
In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.
In taluni caso il documento viene inviato in formato cartaceo attraverso mezzi interni alla amministrazione.

4.3 DOCUMENTO INTERNO FORMALE

I documenti interni sono formati con tecnologie informatiche.
Lo scambio tra UOR di documenti informatici di rilevanza amministrativa giuridico probatoria, avviene di norma per mezzo della posta elettronica convenzionale, o, se disponibile, di quella certificata.
Il documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato.
Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato. In taluni casi il documento in formato digitale viene direttamente allegato al registro di protocollo e da quel momento diventa consultabile direttamente accedendo al sistema di protocollo.
L'operazione appena descritta viene sempre fatta per i documenti in entrata gestiti dalla UOP della Area 3; in questo modo il destinatario del documento ha la possibilità in tempo reale di visualizzarlo e gestirlo attraverso il PdP.

4.4 DOCUMENTO INTERNO INFORMALE

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

4.5 IL DOCUMENTO INFORMATICO

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

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

4.6 IL DOCUMENTO ANALOGICO CARTACEO

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

pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale". Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampata.
In quest'ultimo caso si definisce "*originale*" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e destinatario, stampato su carta intestata e dotato di firma autografa.
Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del Manuale.

4.7 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

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

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

Le firme (e le sigle se si tratta di documento analogico) necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR.
Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

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

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, firma del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo (RPA) e/o del responsabile del provvedimento finale.

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

4.8 SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI

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

4.9 REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO

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

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

4.10 FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.9 è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito www.cnipa.gov.it).

5. Descrizione del flusso di lavorazione dei documenti

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

5.1 GENERALITÀ

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

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

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.
Come previsto dalla normativa vigente i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.
Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.

5.2 Gestione dei documenti

5.2.1 PROVENIENZA ESTERNA DEI DOCUMENTI

I documenti che sono trasmessi da soggetti esterni all'amministrazione(sia personalmente che attraverso il servizio postale) sono recapitati alla Area 1, quindi assegnati sul cartaceo e portati presso la UOP della Area 3.

5.2.2 PROVENIENZA DI DOCUMENTI INTERNI FORMALI

Per sorgente interna dei documenti si intende qualunque RPA che invia formalmente la propria corrispondenza ad altra UOR.
Il documento è di tipo informatico secondo i formati standard illustrati nel precedente capitolo.
I mezzi di recapito della corrispondenza considerati sono la posta elettronica convenzionale o certificata.
Nel caso di trasmissione interna, se al documento sono associati allegati che superano la dimensione della casella di posta elettronica della AOO, si procede ad un riversamento (nelle forme dovute), su supporto rimovibile da consegnare al destinatario del documento, o la trasmissione tramite aree condivise nella intranet della AOO.
Nella fase transitoria verso la diffusione della digitalizzazione dell'amministrazione, i documenti interni possono essere anche di tipo analogico.
In questo caso il mezzo di recapito del documento può essere il servizio di posta interna(raccomandata a libretto).

5.2.3 RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ISTITUZIONALE

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla/e UOP in cui si è organizzata l'AOO. Quando i documenti informatici pervengono alle UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento procede alla registrazione di protocollo.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate. L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.
L'addetto alla gestione della casella di posta elettronica certificata controlla quotidianamente i messaggi pervenuti e verifica se sono da protocollare.

5.2.4 RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ELETTRONICA NON ISTITUZIONALE

Nel caso in cui il messaggio viene ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio viene inoltrato alla casella di posta istituzionale e inviando un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta. I controlli effettuati sul messaggio sono quelli sopra richiamati.

5.2.5 RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI RIMOVIBILI

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

5.2.6 RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE

I documenti pervenuti a mezzo posta o ritirati dal personale della UOP dagli uffici postali sono consegnati alla UOP.
Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.
La corrispondenza relativa a bandi di gara è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza personale non deve essere aperta, né protocollata ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo per la registrazione. La corrispondenza ricevuta via telegramma o via telefax o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo con le modalità descritte nel successivo capitolo 10.
Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.
La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

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

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

chiusura del protocollo, la posta a una delle UOP abilitate e “incaricate” dell’apertura della corrispondenza e della protocollazione.
Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.
Nei casi in cui un UOR non sia stato autorizzato al trattamento dei dati personali ma sia stato abilitato all’uso del servizio telefax e possa ricevere corrispondenza direttamente dall’esterno, avrà cura di non comunicare ai destinatari della corrispondenza il proprio numero di telefax:

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

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

5.2.8 ERRATA RICEZIONE DI DOCUMENTI DIGITALI

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

5.2.9 ERRATA RICEZIONE DI DOCUMENTI CARTACEI

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

- busta indirizzata ad altra AOO della stessa amministrazione:

a) si invia alla AOO corretta;
b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo “documento pervenuto per errore” e si invia alla AOO destinataria apponendo sulla busta la dicitura “Pervenuta ed aperta per errore”;

- busta indirizzata ad altra amministrazione:

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

5.2.10 ATTIVITÀ DI PROTOCOLLAZIONE DEI DOCUMENTI

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e “segnati” nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliate nel capitolo 10.

5.2.11 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI INFORMATICI

La ricezione di documenti comporta l’invio al mittente di due tipologie diverse di ricevute:

- una legata al servizio di posta certificata,
- una al servizio di protocollazione informatica(se richiesto dal mittente).

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.
Nel caso di consegna a mano direttamente alla UOP il mittente può richiede una ricevuta stampata direttamente dal PdP dopo la creazione del relativo protocollo(come descritto al paragrafo successivo).

5.2.12 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI

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

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

5.2.13 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

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

5.2.14 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

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

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

I documenti cartacei dopo l'operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della delibera CNIPA 19 febbraio 2004 n.11 vengono inviati agli UOR/RPA destinatari per le operazioni di fascicolazione e conservazione.
I documenti con più destinatari, sono riprodotti in formato immagine ed inviati solo in formato elettronico. (opzionale Il documento cartaceo originale viene inviato al primo destinatario).
La riproduzione dei documenti cartacei in formato immagine viene eseguita sulla base dei seguenti criteri:

- se il documento ricevuto in formato A4 o A3 non supera le 50 pagine viene acquisito direttamente con le risorse, umane e strumentali, interne all'AOO;
- se il documento ha una consistenza maggiore o formati diversi dai precedenti, viene acquisito in formato immagine solo se esplicitamente richiesto dagli UOR/RPA di competenza, avvalendosi eventualmente dei servizi di una struttura esterna specializzata. In questo caso il RSP, insieme al RPA, individua i documenti da sottoporre al processo di scansione e ne fissa i tempi, diversi da quelli ordinari, e le modalità esecutive.
- In ogni caso non vengono riprodotti in formato immagine i seguenti documenti:
  - i certificati medici contenenti la diagnosi,
  - i progetti ed i loro allegati progettuali,
  - la documentazione relativa a bandi pubblici.

Tutte le UOP hanno a disposizione uno scanner per acquisire documenti in formati digitale.

5.2.15 CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO DEI DOCUMENTI

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

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

5.2.16 CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE

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

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

5.2.17 CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI NELLA FASE CORRENTE

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

5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO

5.3.1 VERIFICA FORMALE DEI DOCUMENTI

Ogni UOR è autorizzata dall'AOO per il tramite del RSP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.
Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR.
Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.
Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo generale o particolare; in caso contrario è restituito al mittente RPA con le osservazioni del caso.

5.3.2 REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UOR abilitati in quanto collegati al sistema di protocollo informatico della AOO a cui appartengono.
Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA. Il documento registrato presso il protocollo riservato è contrassegnato da un lucchetto posto in basso a sinistra del registro di protocollo.

5.3.3 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 di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.
Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

5.3.4 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA

La UOR , per la alla trasmissione “fisica” di un documento in partenza all’interno della amministrazione, consegna il documento già protocollato alla Area 1 Coordinamento che si fa carico attraverso apposito personale della consegna.

5.3.5 AFFRANCATURA DEI DOCUMENTI IN PARTENZA

La Area 1 provvede alle operazioni necessarie per l’invio della corrispondenza in partenza verso soggetti esterni alla amministrazione (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.).
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla Area 1 nelle prime ore del mattino.

5.3.6 CONTEGGI SPEDIZIONE CORRISPONDENZA

L’Ufficio posta della Area 1 effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

5.3.7 DOCUMENTI IN PARTENZA PER POSTA CONVENZIONALE CON PIÙ DESTINATARI

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

5.3.8 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO TELEFAX

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

5.3.9 INSERIMENTO DELLE RICEVUTE DI TRASMISSIONE NEL FASCICOLO

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all’interno del relativo fascicolo.
Gli UOR che effettuano la spedizione di documenti informatici o cartacei direttamente curano anche l’archiviazione delle ricevute di ritorno.

6. Regole di smistamento ed assegnazione dei documenti ricevuti

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

6.1 REGOLE DISPONIBILI CON IL PDP

Le AOO che fruiscono del servizio di protocollo con il proprio PdP eseguono lo smistamento e l’assegnazione dei documenti protocollati e segnati adottando le funzionalità di seguito illustrate:
Tutti i documenti in arrivo alla AOO vengono fisicamente portati presso la Area 1 che li assegna scrivendo sul documento stesso il destinatario interno. Il documento viene quindi consegnato alla Area 3 che si occupa di protocollarlo e trasferirlo tramite assegnazione su iride sulla scrivania della Area/UOB/servizio; da quello momento il documento può essere assegnato dal responsabile della Area/UOB/servizio ad uno o più dei propri collaboratori.
L’attività di smistamento consiste nell’operazione di inviare un documento protocollato e segnato all’UOR competente in base alla classificazione di primo livello del titolario, documento.
Con l’assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione.
Effettuato lo smistamento e l’assegnazione, il RPA provvede alla presa in carico del documento allo stesso assegnato.

Una volta che al mittente iniziale (UOP) giunge notizia di presa in carico della corrispondenza, è cura di questo inviare, con le tecnologie adatte, il documento oggetto di lavorazione compilato nella parte di segnatura (o timbro di segnatura) al UOR/RPA di competenza.
L'assegnazione può essere effettuata per conoscenza o per competenza.
L'UOR competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.
I documenti che sono immediatamente riconducibili ad una specifica UOR e/o materia, vengono inoltrati direttamente dalla UOP.
I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.
Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.
La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.
Nell'allegato 16.3 sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.

6.2 CORRISPONDENZA DI PARTICOLARE RILEVANZA

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione al Dirigente Generale che provvede ad individuare l'UOR competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

6.3 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO DIGITALE

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

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

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

6.4 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO

I documenti ricevuti dall'amministrazione in formato cartaceo vengono acquisiti in formato immagine con l'ausilio di appositi scanner; una volta concluse le operazioni di registrazione, di segnatura e di assegnazione, sono fatti pervenire al RPA di competenza attraverso il caricamento dello stesso allegato sul protocollo informatico. L'originale cartaceo viene essere successivamente trasmesso al RPA. L'UOR competente ha notizia dell'arrivo del documento ad essa indirizzata tramite il sistema di protocollo informatico e tramite l'arrivo del cartaceo.
La "presa in carico" dei documenti informatici viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOR di competenza coincide con la data di assegnazione degli stessi.
I documenti cartacei gestiti dalla UOP sono di norma smistati entro le giornata in cui sono pervenuti, salvo che vi siano eventi eccezionali che impediscano lo smistamento; in questo caso, l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

6.5 MODIFICA DELLE ASSEGNAZIONI

Nel caso di assegnazione errata, l'UOR che riceve il documento comunica l'errore alla UOP che ha erroneamente assegnato il documento, che procederà ad una nuova assegnazione.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

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

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO
In base al modello organizzativo adottato dall'Amministrazione/AOO (si veda il par. 1.4 del presente MdG), nell'allegato 16.3 è riportato, per ciascuna AOO, l'elenco delle unità organizzative responsabili delle attività di registrazione del protocollo (UOP). Relativamente alla organizzazione e alla tenuta dei documenti dell'amministrazione all'interno di ciascuna AOO (o della AOO se unica), sono istituiti il servizio archivistico e eventualmente il servizio per la conservazione sostitutiva e sono definite le strutture dedicate alla conservazione dei documenti.
I servizi in argomento sono stati identificati e formalizzati prima di rendere operativo il servizio di gestione informatica del protocollo, dei documenti e degli archivi.

7.1 SERVIZIO ARCHIVISTICO

L'amministrazione ha istituito il servizio archivistico nell'ambito dell'unica AOO in cui è organizzato il servizio di protocollo e gestione documentale.
Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto servizio per la tenuta del protocollo informatico. Alla guida del servizio archivistico è preposto **il Dirigente della Area 3.**
Nei casi di vacanza, assenza o impedimento del responsabile del servizio archivistico, questo sarà sostituto dal Dirigente/Funzionario più anziano della Area 3.

7.2 SERVIZIO DELLA CONSERVAZIONE ELETTRONICA DEI DOCUMENTI

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

- del protocollo informatico;
- della gestione dei documenti:
  - relative ai fascicoli che fanno riferimento a procedimenti conclusi;
  - riversamento su nuovi supporti informatici per garantire nel tempo la leggibilità dei medesimi.

Il responsabile delle procedure di conservazione sostitutiva, può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone dell'AOO che, per competenza ed esperienza, garantiscano la corretta esecuzione di tali operazioni. L'amministrazione si riserva la facoltà di affidare, in tutto o in parte, ad altri soggetti, pubblici o privati, il procedimento di conservazione e di riversamento; questi sono tenuti ad osservare quanto previsto dalle norme vigenti in materia di protocollo e protezione dei dati personali (integrate, all'occorrenza, da specifici richiami contrattuali).
Nel caso di affidamento a "soggetto esterno", l'amministrazione provvede ad incaricare formalmente tale soggetto (ad esempio Società di servizi, Consulente, ecc) delle attività di conservazione e riversamento e nel contempo lo diffida dal comunicare o diffondere, anche accidentalmente, gli eventuali dati personali comuni, sensibili e/o giudiziari presenti nei supporti oggetto di copia e di riversamento.

7.2.1 ARCHIVIAZIONE OTTICA DEI DOCUMENTI ANALOGICI

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

8. Sistema di classificazione, fascicolazione e piano di conservazione

8.1 PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

8.1.1 GENERALITÀ

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

8.1.2 MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

Gli archivi e i singoli documenti degli enti pubblici non territoriali sono beni culturali inalienabili.
I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.
L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità. Il trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.

8.2 TITOLARIO O PIANO DI CLASSIFICAZIONE

8.2.1 TITOLARIO

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.
L'elenco delle classifiche presenti nel Pdp è diviso per Area/servizio/UOB e permette di classificare il documento in base alla sua tipologia(personale, sicurezza, missioni etc.).
L'utente amministratore è abilitato alle eventuali modifiche o cancellazioni.

8.2.2 CLASSIFICAZIONE DEI DOCUMENTI

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.
Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse, etc.), il numero del fascicolo.
Qualora l'ente lo ritenga opportuno, le operazioni di classificazione possono essere svolte in momenti diversi: l'addetto alla registrazione di protocollo può inserire la voce di livello più alto, mentre l'attribuzione delle voci di dettaglio è demandata all'incaricato della trattazione della pratica.

9. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

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

9.1 UNICITÀ DEL PROTOCOLLO INFORMATICO

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo, centralizzato o distribuito delle UOP, adottato dall'AOO medesima.
La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.
Il numero di protocollo è costituito da sette cifre numeriche.
Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

9.2 REGISTRO GIORNALIERO DI PROTOCOLLO

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, presso un ente certificato per la conservazione sostitutiva.
Tale operazione di riversamento viene fatta in modo automatico dal Pdp correttamente configurato.

9.3 REGISTRAZIONE DI PROTOCOLLO

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).
Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.
Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

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

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.
Tali dati facoltativi sono descritti nei paragrafi seguenti.

9.3.1 DOCUMENTI INFORMATICI

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

9.3.2 DOCUMENTI ANALOGICI (CARTACEI E SUPPORTI RIMOVIBILI)

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

9.5.2 DOCUMENTI CARTACEI

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

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

Facoltativamente possono essere riportate anche le seguenti informazioni:

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

Il "segno" grafico di norma è realizzato con una etichetta autoadesiva corredata di codice a barre o, in alternativa, con un timbro tradizionale.
L'AOO ha optato per il "segno" riportato nell'allegato 16.6.
L'operazione di segnatura dei documenti in partenza viene effettuata dall'UOR/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dalla UOP. L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.
Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo deve essere apposto sulla prima pagina dell'originale;

9.4 ANNULLAMENTO/MODIFICHE DELLE REGISTRAZIONI DI PROTOCOLLO

In caso di errori in fase di inserimento l'utente amministratore è abilitato(dietro richiesta scritta inviata via mail) alla modifica di alcuni elementi del protocollo(Oggetto, classifica ecc.).
In casi particolari l'utente amministratore(dietro richiesta scritta e motivata inviata via mail) può annullare definitivamente il numero di protocollo che da quel momento non sarà più disponibile e comparirà sul prtocollo come annullato con la relativa motivazione.
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.

9.5 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

9.5.1 REGISTRAZIONI DI PROTOCOLLO PARTICOLARI (RISERVATE)

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

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

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

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

9.5.2 CIRCOLARI E DISPOSIZIONI GENERALI

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.
I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

9.5.3 DOCUMENTI CARTACEI IN PARTENZA CON PIÙ DESTINATARI

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica.
L'elenco dei destinatari, in formato cartaceo, viene allegato alla minuta dell'originale.

9.5.4 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.
Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.
L'accertamento della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.
Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RPA provvede ad acquisire l'originale.
Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "Già pervenuto via fax il giorno……..".
Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso.
Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione. Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax".
Il documento in partenza reca una delle seguenti diciture:

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

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

9.5.5 PROTOCOLLAZIONE DI UN NUMERO CONSISTENTE DI DOCUMENTI CARTACEI

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

9.5.6 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, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

9.5.7 PROTOCOLLAZIONE DI DOCUMENTI INERENTI A GARE DI APPALTO CONFEZIONATI SU SUPPORTI CARTACEI

La corrispondenza che riporta l'indicazione "offerta" "gara d'appalto" "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.
Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

9.5.8 PROTOCOLLI URGENTI

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.
Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da spedire.
Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'UOP.

9.5.9 DOCUMENTI NON FIRMATI

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.
Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.
È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

9.5.10 PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

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

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

9.5.11 PROTOCOLLO DI DOCUMENTI DIGITALI PERVENUTI ERRONEAMENTE

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

9.5.12 RICEZIONE DI DOCUMENTI CARTACEI PERVENUTI ERRONEAMENTE

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

9.5.13 COPIE PER CONOSCENZA

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 10.8.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.
Tale informazione è riportata anche sulla segnatura di protocollo.

9.5.14 CORRISPONDENZA PERSONALE O RISERVATA

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

9.5.15 INTEGRAZIONI DOCUMENTARIE

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.
Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

9.6 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL PDP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il PdP.
Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

9.7 REGISTRAZIONI DI PROTOCOLLO

9.7.1 ATTRIBUZIONE DEL PROTOCOLLO

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il servizio di protocollo è realizzato dall'applicativo PdP attraverso l'apposizione di un riferimento temporale come previsto dalla normativa vigente.
Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

- Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili e giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

9.7.2 REGISTRO GIORNALIERO DI PROTOCOLLO(DPCM 3/12/2013)

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

- estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di protocollo;
- riversamento nell'apposito spazio web concordato con il fornitore della coservazione sostituitiva dei documenti digitali;

- copia del file nello storage presente all'interno della AOO;

L'ufficio o l'addetto incaricato di eseguire tali operazione è stato individuato dal RSP.
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

10. SISTEMA DI PDP IN USO ALLA AOO

il Dipartimento della programmazione utilizza per tutte le operazioni relative al protocollo informatico il sistema Iride. Tale sistema è stato prodotto dalla Società Cedaf di Forlì ed è gestito dalla società Sicilia Digitale.
Il manuale di funzionamento del sistema Iride è reperibile sul sito istituzionale http://pti.regione.sicilia.it/.

11. Rilascio delle abilitazioni di accesso alle informazioni documentali

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

11.1 GENERALITÀ

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

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

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

• In fase di creazione delle utenze viene assegnato uno o più ruoli che corrispondono alle diverse operazione che il nuovo utente può svolgere sul protocollo.
Al nuovo utente viene assegnata la possibilità di inserire nuovi protocolli o lavorare quelli già esistenti all'interno della Area/UOB/servizio nel quale è incardinato. Nel caso di esigenze particolari possono essere richiesti può ruoli o autorizzazioni particolari inviando una apposita richiesta all'amministratore del protocollo.

11.2 ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO

Gli utenti abilitati accedono al PdP **attraverso il nome utente e la password che gli sono state comunicate via mail. L'utente deve immediatamente modificare la password provvisoria che gli è stata asssegnata.**
Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.
Il "file delle password" utilizzato dal servizio di accesso è una tabella presente all'interno del server che ospita il protocollo informatico e accessibile soltanto da un processo di sistema ed in ogni caso le password sono criptate e non visibili da nessuno

11.3 PROFILI DI ACCESSO

11.3.1 UTENTE AMMINISTRATORE DI PDP

L'utente amministratore o gli utenti amministratori fanno capo alla Area 3 del Dipartimento Programmazione.
Tale utente è abilitato a svolgere tutte le funzioni di amministrazione relative al PDP e dietro richiesta scritta può sia modificare che annullare un numero di protocollo.
Inoltre esistono delle credenziali da amministratore presso Sicilia Digitale che vengono utilizzate per interventi di manutenzione ed aggiornamento del sistema.

11.3.2 OPERATORE DI PROTOCOLLO

L'utente operatore è l'unico autorizzato a protocollare documenti in arrivo secondo le modalità ampiamente descritte.
L'Area 3 e a l'Area1 del Dipartimento Programmazione hanno utenti abilitati a tale ruolo.

11.3.3 UTENTE ORDINARIO

L'utente ordinario può effettuare tutte le operazione di visualizzazione e gestione delle pratiche inerenti il protocollo

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

Al fine di procedere alla creazione delle utenze dovrà essere presentata formale richiesta da parte dei responsabili delle strutture intermedie inserite nell'AOO di competenza.
In caso di smarrimento della password, dovrà essere presentata formale richiesta da parte dei responsabili delle strutture intermedie inserite nell'AOO di competenza; in questo caso l'utente amministratore ha la possibilità di resettare la password senza, in ogni caso, vedere la vecchia.

11.5 CONSULTAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO PARTICOLARI

Il complesso dei documenti per i quali è stata attivata la registrazione di protocollo particolare costituisce l'archivio particolare.
I documenti e i fascicoli dell'archivio particolare sono consultabili nel rispetto delle seguenti norme:

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

12. Modalità di utilizzo del registro di emergenza

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

12.1 IL REGISTRO DI EMERGENZA

Qualora non fosse disponibile fruire del PdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.
Il registro di emergenza viene istituito ogni volta che il PdP non è accessibile.
Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale.
Il registro di emergenza si configura come un repertorio del protocollo generale.
Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.
A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.
In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo

12.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

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

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

12.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.
Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo generale.
Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico (o persona da lui delegata) provvede a tener informato il RSP sui tempi di ripristino del servizio

12.4 MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA

È compito del RSP verificare la chiusura del registro di emergenza.
È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.
Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza (postazione di lavoro stand alone) a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza su una o più postazioni di lavoro dedicate della AOO, sono inserite nel sistema informatico di protocollo generale, utilizzando un'apposita funzione di recupero dei dati).
Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

13 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

L'amministrazione adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico (RSP).
Il presente Manuale potrà essere aggiornato a seguito di:

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

13.1 REGOLAMENTI ABROGATI

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

13.2 PUBBLICITÀ DEL PRESENTE MANUALE

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

13.3 OPERATIVITÀ DEL PRESENTE MANUALE

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

14. Allegati

14.1 DEFINIZIONI

Oggetto/Soggetto	Descrizione
AMMINISTRAZIONI CERTIFICANTI	Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti (art. 1, comma 1, lett. p) del DPR n. 445/2000);
AMMINISTRAZIONI PROCEDENTI	Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio (art. 1, comma 1 lett. o) DPR n. 445/2000);
AMMINISTRAZIONI PUBBLICHE	Per amministrazioni pubbliche si intendono quelle indicate nell'art. 1, comma 2 del d. lgs. 30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI	Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (art. 1, comma 1 lett. z) del d. lgs.7 marzo 2005, n. 82);
ARCHIVIO	L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dell'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione o dalla Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio viene suddiviso in tre sezioni: corrente, di deposito e storica;
ARCHIVIO CORRENTE	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;
ARCHIVIO DI DEPOSITO	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;
ARCHIVIO STORICO	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne;
ARCHIVIAZIONE ELETTRONICA	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (art. 1 della Deliberazione CNIPA 19 febbraio 2004 n. 11);

AREA ORGANIZZATIVA OMOGENEA (AOO)	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato (art. 2, lett. n) del DPCM 31 ottobre 2000);
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (art. 1, comma 1, lett. i) del DPR 28 dicembre 2000, n. 445);
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; (art. 1, comma 1 lett. b) del d. lgs.7 marzo 2005, n. 82);
BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art. 4 comma 1 lett. o) del d. lgs. 30 giugno 2003 n. 196);
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (art. 4, comma 1, lett. d) del d. lgs. 30 giugno 2003 n. 196);
CARTA NAZIONALE DEI SERVIZI	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (art. 1 del d. lgs.7 marzo 2005, n. 82);
CARTA D'IDENTITÀ ELETTRONICA	Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare (art. 1 comma 1, lett. c) del d. lgs.7 marzo 2005, n. 82);
CASELLA DI POSTA ELETTRONICA ISTITUZIONALE	La casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del DPCM 31 ottobre 2000, articolo 15, comma 3). (art. 1 dell'allegato A alla circolare AIPA 7 maggio 2001 n. 28);
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (art. 1, comma 1 lett. e) del d. lgs.7 marzo 2005, n. 82);
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art. 1 comma 1 lett. f) del d. lgs.7 marzo 2005, n. 82);
CERTIFICATO	Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (art. 1 comma 1 lett. f) del DPR 28 dicembre 2000, n. 445);
CERTIFICATORE	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art. 1, comma 1 lett. g) del d. lgs. 7 marzo 2005, n. 82);
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione.

COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 comma 1 lett. l) del d. lgs. 30 giugno 2003 n. 196);
CONSERVAZIONE SOSTITUTIVA	Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004, n.11;
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art. 4 comma 3 lett. d) del d. lgs. 30 giugno 2003 n. 196);
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4, comma 1 lett. e) del d. lgs. 30 giugno 2003 n. 196);
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato (art. 4, comma 1 lett. c) del d. lgs. 30 giugno 2003 n. 196);
DATI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4 comma 1, lett. ddd) del d. lgs. 30 giugno 2003 n. 196);
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art. 4 comma 1 lett. n) del d. lgs. 30 giugno 2003 n. 196);
DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4 comma 1 lett. b) del d. lgs. 30 giugno 2003 n. 196);
DATO PUBBLICO	Il dato conoscibile da chiunque (art. 1 comma 1 lett. n) del d. lgs. 7 marzo 2005, n. 82);
DATO A CONOSCIBLITÀ LIMITATA	Il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. 1 comma 1 lett. l) del d. lgs.7 marzo 2005, n. 82);
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dall' art. 1 comma 1 lett. h) del DPR 28 dicembre 2000, n. 445;
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato (art. 1 comma 1 lett. g) del DPR 28 dicembre 2000, n. 445);
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 del d. lgs. 30 giugno 2003 n. 196);
DOCUMENTO	Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (art. 1 comma 1 lett. a) Deliberazione CNIPA del 19 febbraio 2004 n.11);

DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (art. 1 comma 1 lett. a) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO ANALOGICO	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art. 1 comma 1 lett. b) Deliberazione CNIPA del 19 febbraio 2004, n.11);
DOCUMENTO ANALOGICO ORIGINALE	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (art. 1 comma 1 lett. h) Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO CONSERVATO	Documento sottoposto al processo di conservazione sostitutiva (art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare. (art. 1 comma 1 lett. c) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare (art. 1 comma 1 lett. d) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITÀ ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (art. 1 comma 1 lett. e) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. t) del d. lgs.7 marzo 2005, n. 82);
DOSSIER	È una aggregazione di più fascicoli che può essere costituita a seguito di esigenze operative dell'Amministrazione, come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona;
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia (art. 1 comma 1 lett. n) della deliberazione AIPA 19 febbraio 2004 n. 11);
EVIDENZA INFORMATICA FASCICOLAZIONE FASCICOLO	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1 comma 1, lett. f) del DPCM 13 gennaio 2004);
FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.

FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento;
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lett. s) del d. lgs.7 marzo 2005, n. 82);
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lett. q) del d. lgs.7 marzo 2005, n. 82);
FIRMA ELETTRONICA QUALIFICATA	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1 comma 1 lett. r) del d. lgs.7 marzo 2005, n. 82);
FORMAZIONE DEI DOCUMENTI INFORMATICI	Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa (art. 2 della deliberazione AIPA 23 novembre 2000 n. 51);
FUNZIONE DI HASH	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (art. 1 comma 1 lett. e) del DPCM 13 gennaio 2004);
GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del d. lgs. 30 giugno 2003 n. 196, istituita dalla legge 31 dicembre 1996, n. 675 (art. 4 comma 1 lett. q) del d. lgs. 30 giugno 2003 n. 196);
GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1 comma 1 lett. l) del d. lgs. 7 marzo 2005, n. 82);

IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art. 1 del DPCM 13 geo 2004);
INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
INSERTO	È un sottoinsieme omogeneo del sotto fascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (art. 1 comma 1 lett. l) del DPR 28 dicembre 2000, n. 445);
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato (art. 1 comma 1 lett. n) del DPR 28 dicembre 2000, n. 445);
MARCA TEMPORALE	Un'evidenza informatica che consente la validazione temporale (art. 1 comma 1 lett. i) del DPCM 31 gennaio 2004);
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sotto partizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascun procedimento/procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello Stato o per la sezione degli archivi storici per gli Enti pubblici) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il PIANO DI CONSERVAZIONE periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
MEMORIZZAZIONE	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del decreto legislativo 23 gennaio 2002, n. 10 (art 1, comma 1, lett. f) Deliberazione CNIPA del 19 febbraio 2004 n.11);
MISURE MINIME DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del d. lgs. 30 giugno 2003 n. 196 (art. 4 comma 3 lett. a) del d. lgs. 30 giugno 2003 n. 196);
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica (art. 4, comma 3, lett. e) del d. lgs. 30 giugno 2003, n. 196);
ORIGINALI NON UNICI	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1, comma 1, lett. v) del d. lgs. 7 marzo 2005, n. 82);
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	Vedi MASSIMARO DI SELEZIONE E SCARTO

PROFILO DI AUTORIZZAZIONE	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (art. 4, comma 3, lett. f) del d. lgs. 30 giugno 2003 n. 196);
PUBBLICO UFFICIALE	Il notaio, salvo quanto previsto dall'art. 5, comma 4 della Deliberazione CNIPA del 19 febbraio 2004, n. 11 e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (art. 1 Deliberazione CNIPA del 19 febbraio 2004, n. 11);
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, comma 1, lett. g) del d. lgs. 30 giugno 2003 n. 196);
RESPONSABILE DEL SERVIZIO DI PROTOCOLLO	Il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'articolo 62, comma 2, del DPR 28 dicembre 2000, n. 445;
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI (RPA)	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente;
RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art 1, comma 1, lett. g) del DPCM 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (art. 1, comma 1, lett. i), del DPR 11 febbraio 2005, n. 68);
RIVERSAMENTO DIRETTO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (art. comma 1, lett. l) Deliberazione CNIPA del 19 febbraio 2004, n. 11)
RIVERSAMENTO SOSTITUTIVO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (art. 1, comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11)
SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (art. 4, comma 4, lett. c) del d. lgs. 30 giugno 2003 n. 196);
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (art. 4, comma 4, lett. b) del d. lgs. 30 giugno 2003 n. 196);
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (art. 4, comma 4, lett. a) del d. lgs. 30 giugno 2003 n. 196);
SEGNATURA INFORMATICA	L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'articolo 18, comma 1, del DPCM 31 ottobre 2000 (art. 1 dell'allegato A della circolare AIPA 7 maggio 2001 n. 28);
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (Glossario dell'IPA Indice delle Pubbliche Amministrazioni);

SISTEMA DI CLASSIFICAZIONE	Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (art. 2, comma 1, lett. h) del DPCM 31 ottobre 2000);
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art. 4, comma 3, lett. g) del d. lgs. 30 giugno 2003 n. 196);
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1, comma 1, lett. r) del DPR 28 dicembre 2000 n. 445);
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati.

14.2 NORMATIVA DI RIFERIMENTO

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

16. Decreto legislativo 23 gennaio 2002, n. 10 Recepimento della direttiva 1999/93/CE sulla firma elettronica.
17. Direttiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002 -Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
18. Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002 Linee guida in materia di digitalizzazione dell'amministrazione.
19. Legge 27 dicembre 2002, n. 289 Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
20. DPR 7 aprile 2003, n. 137 Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002.
21. Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali.
22. Decreto Ministeriale 14 ottobre 2003 Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23. Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003 Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
24. Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003.
25. Direttiva 18 dicembre 2003 Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
26. DPCM 13 gennaio 2004 Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98)
27. Deliberazione CNIPA 19 febbraio 2004, n. 11 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
28. Decreto legislativo 22 gennaio 2004, n. 42 Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28).

14.3 AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO

14.3.1 MODELLO ORGANIZZATIVO DELL'AMMINISTRAZIONE

Denominazione dell'Amministrazione	DIPARTIMENTO REGIONALE DELLA PROGRAMMAZIONE
Codice identificativo assegnato all'Amministrazione	//
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	PIAZZA STURZO 36 90139 PALERMO
Elenco delle AREE ORGANIZZATIVE OMOGENEE – AOO	AOO1 (Dipartimento programmazione)

14.3.2 CARATTERIZZAZIONE DI CIASCUNA AREA ORGANIZZATIVA OMOGENEA

Denominazione dell'Area Organizzativa Omogenea	DIPARTIMENTO PROGRAMMAZIONE
Codice identificativo assegnato alla AOO	AOO1
Nominativo del Responsabile del Servizio di Protocollo informatico, gestione documentale e archivistica	Ing. Eugenio Patricolo
Casella di posta elettronica istituzionale dell'AOO (1)	dipartimento.programmazione@regione.sicilia.it
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale	DIPARTIMENTO PROGRAMMAZIONE – PIAZZA STURZO 36 90139 PALERMO
Data di istituzione della AOO	17/05/2006
Data di soppressione della AOO	XXX

Data di migrazione della AOO verso Sicilia Digitale	11/11/2019	
Articolazione della AOO in Unità Organizzative di registrazione di Protocollo UOP	AREA 1 – UFFICIO DI SUPPORTO E COORDINAMENTO DEL DIRIGENTE GENERALE – ANTICORRUZIONE – CONTENZIOSO – COORDINAMENTO NUCLEO DI VALUTAZIONE E VERIFICA DEGLI INVESTIMENTI PUBBLICI Tipo protocollazione:	-Arrivo -interno -partenza
	AREA 3-AFFARI GENERALI, PERSONALE, CONTENZIOSO E BILANCIO Tipo protocollazione:	-Arrivo -interno -partenza
Articolazione della AOO in Uffici Organizzativi di Riferimento - UOR	UNITA' DI STAFF 1 – UFFICIO DEL CONTROLLO INTERNO DI GESTIONE	-interno -partenza
	UNITA' DI STAFF 2 – ADEMPIMENTI CONNESSI ALLA FUNZIONE DI AUTORITÀ DI GESTIONE	-interno -partenza
	AREA 1 – UFFICIO DI SUPPORTO E COORDINAMENTO DEL DIRIGENTE GENERALE – ANTICORRUZIONE – CONTENZIOSO – COORDINAMENTO NUCLEO DI VALUTAZIONE E VERIFICA DEGLI INVESTIMENTI PUBBLICI	-Arrivo -interno -partenza
	U.O.B. A1.1 - COORDINAMENTO NUCLEO DI VALUTAZIONE E VERIFICA DEGLI INVESTIMENTI PUBBLICI	-interno -partenza
	AREA 2 – COORDINAMENTO MONITORAGGIO PROGRAMMI COMUNITARI E NAZIONALI	-interno -partenza
	U.O.B. A2.1 - SISTEMA INFORMATIVO - MONITORAGGIO PROGRAMMI ITALIA/MALTA, ITALIA/TUNISIA	-interno -partenza
	AREA 3 – AFFARI GENERALI – PERSONALE – BILANCIO – COMUNICAZIONE – TRASPARENZA – CONTRATTI	-Arrivo -interno -partenza
	U.O.B. A3.01 – Comunicazione – U.R.P.	-interno -partenza
	AREA 4 – ASSISTENZA TECNICA	-interno -partenza
	AREA 5 – PROGRAMMI COMUNITARI E NAZIONALI	-interno -partenza
	U.O.B. A5.01 – Fondo Sviluppo e Coesione	-interno -partenza
	AREA 6 – SVILUPPO URBANO E TERRITORIALE	-interno -partenza
	U.O.B. A6.1 - Sviluppo territoriale e Sviluppo Urbano	-interno -partenza
	AREA 7 – CONTROLLI – REPRESSIONI FRODI COMUNITARIE – CHIUSURA PROGRAMMI COMUNITARI	-interno -partenza
	U.O.B. A7.1 – U.M.C. Autorità di Gestione - Irregolarità e Repressioni frodi nei Programmi Nazionali e Comunitari	-interno -partenza
	SERVIZIO 1 – PROGRAMMAZIONE E COORDINAMENTO POLITICHE DELLE INFRASTRUTTURE, PER I TRASPORTI E MOBILITA', PER ENERGIA E RIFIUTI	-interno -partenza
	U.O.B. S1.1 - Interventi Infrastrutturali	-interno -partenza
	U.O.B. S1.2-INT. INFR. NEL SETTORE DEI RIFIUTI E NEL SETT. ENERGIA	-interno -partenza
	SERVIZIO 2 – PROGRAMMAZIONE E COORDINAMENTO POLITICHE PER RISORSE IDRICHE, TUTELA AMBIENTALE, VALORIZZAZIONE DEI BENI CULTURALI - NATURALI E TURISMO	-interno -partenza

	U.O.B. S2.01 – Attrattori naturali, culturali e turismo	-interno -partenza
	SERVIZIO 3 – PROGRAMMAZIONE E COORDINAMENTO STRATEGIA DELL'INNOVAZIONE, POLITICHE DELLA RICERCA E SVILUPPO, AGENDA DIGITALE E COMPETITIVITÀ DELLE IMPRESE	-interno -partenza
	U.O.B. S3.01 – Ricerca e Sviluppo, Agenda digitale e Competitività dei sistemi produttivi	-interno -partenza
	SERVIZIO 4 – PROGRAMMAZIONE E COORDINAMENTO DELLE POLITICHE PER LE RISORSE UMANE, L'ISTRUZIONE, LE POLITICHE SOCIALI E SANITARIE, LE PARI OPPORTUNITÀ E LA LEGALITÀ	-interno -partenza
	U.O.B. S4.01 – Istruzione, edilizia scolastica ed universitaria	-interno -partenza
	SERVIZIO 5 – COOPERAZIONE TERRITORIALE - PROGRAMMA OPERATIVO CONGIUNTO ENI ITALIA-TUNISIA	-interno -partenza
	SERVIZIO 6 – COOPERAZIONE TERRITORIALE EUROPEA – PROGRAMMA INTERREG V-A ITALIA MALTA	-interno -partenza

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

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

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

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

Decreto del Dirigente Generale **n. 1 del 11/01/2017**

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

14.5 ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE NOMINATIVO TITOLO/RUOLO NELL'AOO ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA

NOMINATIVO	TITOLO/RUOLO NELLA AOO	ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA
Ing. Eugenio Patricolo	RSP	
Dario Tornabene	Dirigente Generale	
Giuseppe Indorante	Utente	
Giovanni Sarri	Utente	
Antonio Costantino	Utente	
Daniela Bica	Utente	
Antonella Vallone	Utente	
Nicola Tarantino	Utente	
Gianfranco Di Liberto	Utente	

Marco Tornambè	Utente	
Franco Badami	Utente	
Vincenzo Falletta	Utente	
Maria Basile	Utente	
Paola Pendino	Utente	
Claudio Basso	Utente	
Piera Anna Maria Spanò	Utente	
Vincenzo Petruso	Utente	

14.6 TIMBRO DI ARRIVO PER LA CORRISPONDENZA CARTACEA IN INGRESSO

A tutti i documenti cartacei in arrivo recapitati alla UOP della Area 3, dopo essere stati protocollati, viene apposta una etichetta (5cm x 3cm) direttamente stampata dal sistema Iride attraverso la funzione timbro.
Questa etichetta riporta la dicitura Dipartimento Programmazione, il numero di protocollo, la data di inserimento e la UOR di destinazione.

Sommario