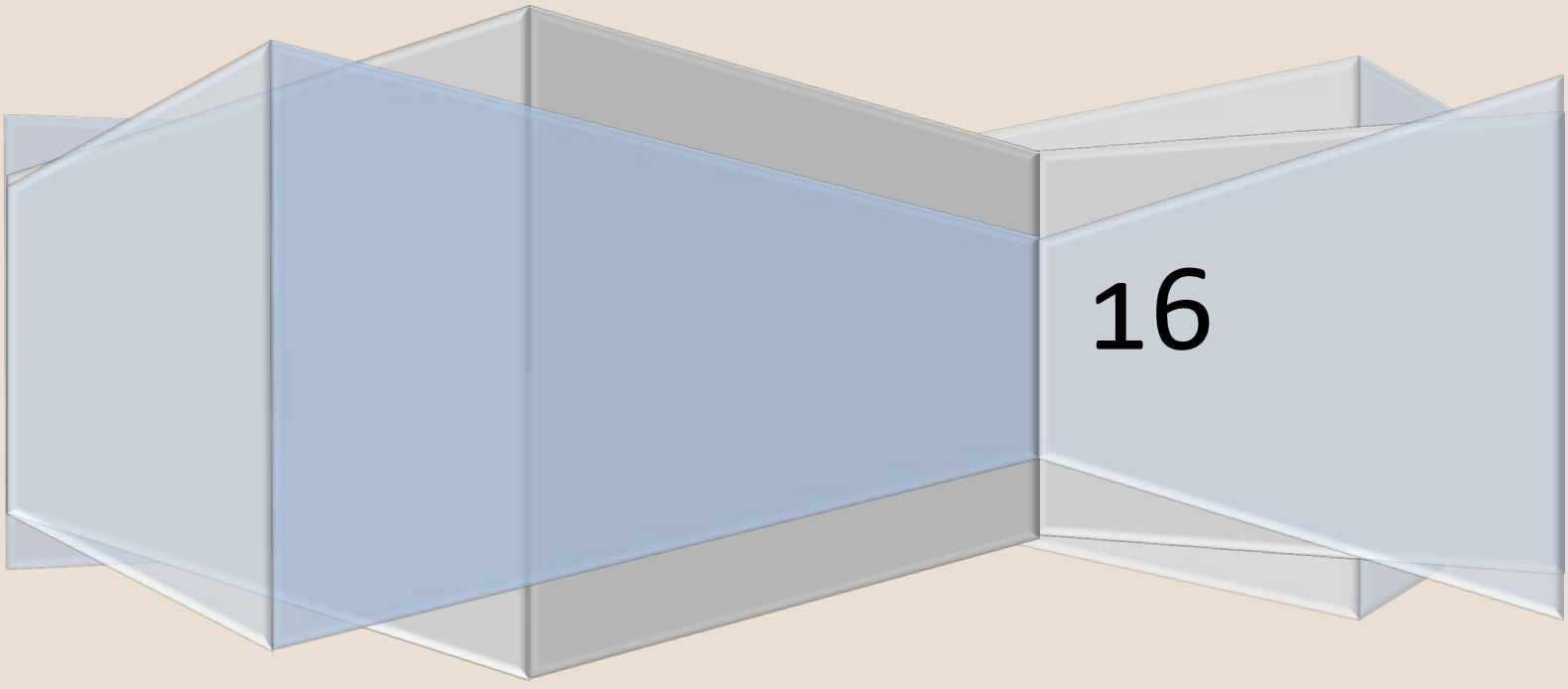
Ministero dell'Istruzione, dell' Università e della Ricerca
ISTITUTO DI ISTRUZIONE SUPERIORE "Giovanni Falcone"
Istituto Profess.le per i Servizi Commerciali, Turistici, Sociali e della Grafica Pubblicitaria
Istituto Tecnico Turistico
Via Levadello – 25036 Palazzolo sull'Oglio (BS)
Tel. 0307405911 – fax 0307401226 – C.F. 91001910172
www.falconeiis.gov.it – email: BSIS03400L@istruzione.it

Manuale di Gestione documentale

Manuale del protocollo informatico ed allegati

deliberato dal C.I. del. n. 1183 Verbale n. 203 del 28.06.2016



Sommario

Ministero dell'Istruzione, dell' Università e della Ricerca
ISTITUTO DI ISTRUZIONE SUPERIORE "Giovanni Falcone"
Istituto Profess.le per i Servizi Commerciali, Turistici, Sociali e della Grafica Pubblicitaria
Istituto Tecnico Turistico
Via Levadello – 25036 Palazzolo sull'Oglio (BS)
Tel. 0307405911 – fax 0307401226 – C.F. 91001910172
www.falconeiis.gov.it – email: BSIS03400L@istruzione.it

Manuale di Gestione del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

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 n. 428", all'art. 3, comma 1, lettera c) – come confermato dal decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" – prevede per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del Manuale di gestione del Protocollo.

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

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa decreto – del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DPR n. 428 del 20 ottobre 1998).

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

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

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Esso disciplina:

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

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

1.2 AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 e successive modificazioni ed integrazioni, 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 dell'amministrazione.

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", RC GIOVANNI FALCONE;
- 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 3 dicembre 2013 Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- per Codice, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale – come integrato e corretto nel decreto legislativo 235/2010

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 all'amministrazione /AOO per implementare il servizio di protocollo informatico;
- **UOP** Unità Organizzative di registrazione di Protocollo – rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** Uffici Organizzativi di Riferimento – un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** Ufficio Utente – un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le Norme ed i Regolamenti di riferimento vedasi l'elenco riportato in *Normativa di riferimento*, nell'allegato al presente MdG

1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO), composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato in *area organizzativa omogena e modello organizzativo*, allegato al presente MdG.
All'interno della AOO il sistema di protocollazione è unico.
Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO
e l'insieme degli UOR che la compongono con la loro articolazione in UU.

All'interno della AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto ogni UOR svolge anche i compiti di UOP.

L'allegato *area organizzativa omogena e modello organizzativo* è suscettibile di modifica in caso di inserimento di nuove UOP/UOR/UU o di riorganizzazione delle medesime.
Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali.
L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UOR allo svolgimento dell'attività di protocollazione.
Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del responsabile del protocollo informatico. Nelle UOR sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

1.5 SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

In ogni AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).
Egli è funzionalmente individuato, e nominato con atto riportato nell'allegato del MdG *Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.*
Al servizio è preposto un dirigente ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.
L'atto che istituisce il servizio e individua il responsabile per ciascuna AOO è riportato nell'allegato indicato, unitamente:

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

È compito del servizio:

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

1.6 CONSERVAZIONE DEI DOCUMENTI

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, entro la giornata lavorativa successiva, come previsto dal DPCM del 3 dicembre 2013 viene inviato al conservatore accreditato incaricato del servizio.
Le procedure di riversamento, predisposte dal RSP, sono illustrate nel piano di sicurezza del MdG.

1.7 FIRMA DIGITALE

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

1.8 TUTELA DEI DATI PERSONALI

L'amministrazione titolare dei dati di protocollo e dei dati personali comuni, sensibili e/o giudiziari contenuti nella documentazione amministrativa di propria pertinenza dà

attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

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

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 3.

In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

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

1.9 CASELLE DI POSTA ELETTRONICA

L'AOO si dota di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento. Inoltre l'AOO si dota di una casella di posta elettronica anche di tipo tradizionale – interna, di appoggio, destinata a raccogliere tutti messaggi con annessi documenti ed eventuali allegati destinati ad essere formalmente inviati all'esterno con la casella di posta "istituzionale" della AOO

1.10 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

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

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

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico. Il contenuto della classificazione è dettagliatamente illustrato nel successivo capitolo 9.

1.11 FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro

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

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

Tali iniziative formative, destinate a specialisti, funzionari e dirigenti sono riportate nell'allegato *Piano Formativo per il personale*

1.12 PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dai DPCM 3/12/2013 e 13/11/2014.
Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunica all'AGID le procedure integrative che intende adottare ai sensi dell'art. 7 della deliberazione CNIPA n. 11/2004.

2. Eliminazione dei protocolli diversi dal protocollo informatico

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

2.1 PIANO DI ATTUAZIONE

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

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

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

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

3.2 GENERALITÀ

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

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, *di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali* e le successive modifiche e integrazioni, 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 accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;

- cambio delle password con frequenza almeno quadrimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento sia alla esecuzione del versamento dei dati in conservazione sostitutiva, sia alla capacità di ripristino del sistema informatico entro sette giorni in caso di disastro;
- conservazione, a cura di Aruba Posta Elettronica Certificata SPA, dei dati e dei documenti secondo le norme stabilite dal decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 e le successive modifiche e integrazioni;
- 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;
- uso di codici identificativi dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. Tali operazioni possono essere delegate a operatori esterni autorizzati o essere automatizzati dal PdP.

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 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, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e

della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui ai DPCM 13 gennaio 2004, 3 dicembre 2013, 13 novembre 2014 e le successive integrazioni. L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza.

3.4 GESTIONE DEI DOCUMENTI INFORMATICI

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

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

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

3.4.1 COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.
Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

Ogni utente viene riconosciuto nel sistema informatico in base a delle credenziali e viene garantito l'accesso alle sezioni del PdP tramite una profilatura multilivellare, che permette di assegnare ad ogni utente l'accesso e la visualizzazione solo dei documenti permessi, come

previsto dall'art. 7 del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, *Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

In relazione alla componente fisica della sicurezza si segnala che i documenti fisici sono salvati in serverfarm esterne, la cui protezione è affidata al gestore del servizio.

3.4.2 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;
- dalle registrazioni del PdP.

- Le registrazioni di sicurezza sono soggette alle seguenti misure:

- Backup giornaliero dei log degli accessi e delle operazioni
- Creazione del registro protocollo giornaliero

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

3.5 TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

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

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 AGID del 23 gennaio 2013, n. 60.

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.

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 e l'eliminazione del documento.

Il PdP adottato dall'amministrazione/AOO:

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

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

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:
Il RSP ha il permesso di creare, modificare e associare agli utenti dei profili di sicurezza a livello di sotto area, garantendone quindi la visualizzazione o la modifica secondo i criteri stabiliti dal RSP stesso.

3.6.2 ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

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

- verifica delle credenziali all'accesso al PdP.
- controllo dei profili ad ogni azione dell'utente.

La visibilità completa sul registro di protocollo è consentita solo agli utenti con il permesso di Gestione completa e profilati per la visualizzazione dei documenti riservati. Questi utenti hanno il permesso di operare al di sopra di tutte le aree e posso assegnare i documenti agli UOP.
L'utente assegnatario dei documenti protocollati è invece abilitato alla visualizzazione e all'archiviazione del documento.
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa del documento stesso è possibile solo a coloro il cui accesso garantisce la visualizzazione dei documenti riservati.
Tutti gli altri utenti possono accedere solo ai dati di registrazione e non possono accedere alla visione del documento.

3.6.3 UTENTI ESTERNI ALLA AOO PRIVATI

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

3.7 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 e le successive integrazioni.

3.7.1 SERVIZIO DI CONSERVAZIONE SOSTITUTIVA

Il responsabile della conservazione sostitutiva dei documenti fornisce le disposizioni, in

sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RSP, per una corretta esecuzione delle operazioni di salvataggio dei dati.
Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione, 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;

3.8 POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

Le politiche di sicurezza, riportate nell'allegato omonimo, stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informatico, sia le misure per la gestione degli incidenti informatici.
Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.
È compito del RSP 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 dall'AGID o a seguito dei risultati delle attività di *audit*.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

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

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

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

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

- informatico;
- analogico.

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

4.1 DOCUMENTO RICEVUTO

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

1. a mezzo posta elettronica convenzionale o certificata;
2. tramite intranet
3. su supporto rimovibile quale, ad esempio, *CD ROM, DVD, floppy disk, tape, pen drive*, etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

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

4.2 DOCUMENTO INVIATO

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

4.3 DOCUMENTO INTERNO FORMALE

I documenti interni sono formati con tecnologie informatiche e sottoposti a protocollazione ed archiviazione

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 30 dicembre 2010, n. 235, recante "Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69." prevede che:

"1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti a tutti gli effetti di legge, ai sensi delle disposizioni del presente codice.
1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

2 [abrogato]

3. Le regole tecniche per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico".

4.6 IL DOCUMENTO ANALOGICO CARTACEO

Per documento analogico si intende un documento amministrativo "*formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale*". Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale

(come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampato.
In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e destinatario, stampato su carta intestata e dotato di firma autografa.
Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del Manuale.

4.7 FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

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

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

Le 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 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 degli allegati, se presenti;
- l'oggetto del documento;
- e trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo (RPA) e/o del responsabile del provvedimento finale.

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

4.8 SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

L'amministrazione, quando non si configura come autorità di certificazione, si avvale dei servizi di una autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'AGID.
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;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP/UOR e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

4.10 FIRMA DIGITALE

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

4.11 USO DELLA POSTA ELETTRONICA CERTIFICATA

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici).
Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato

digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

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

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

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

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

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.
Il servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.
Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi.
La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

5. Descrizione del flusso di lavorazione dei documenti

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

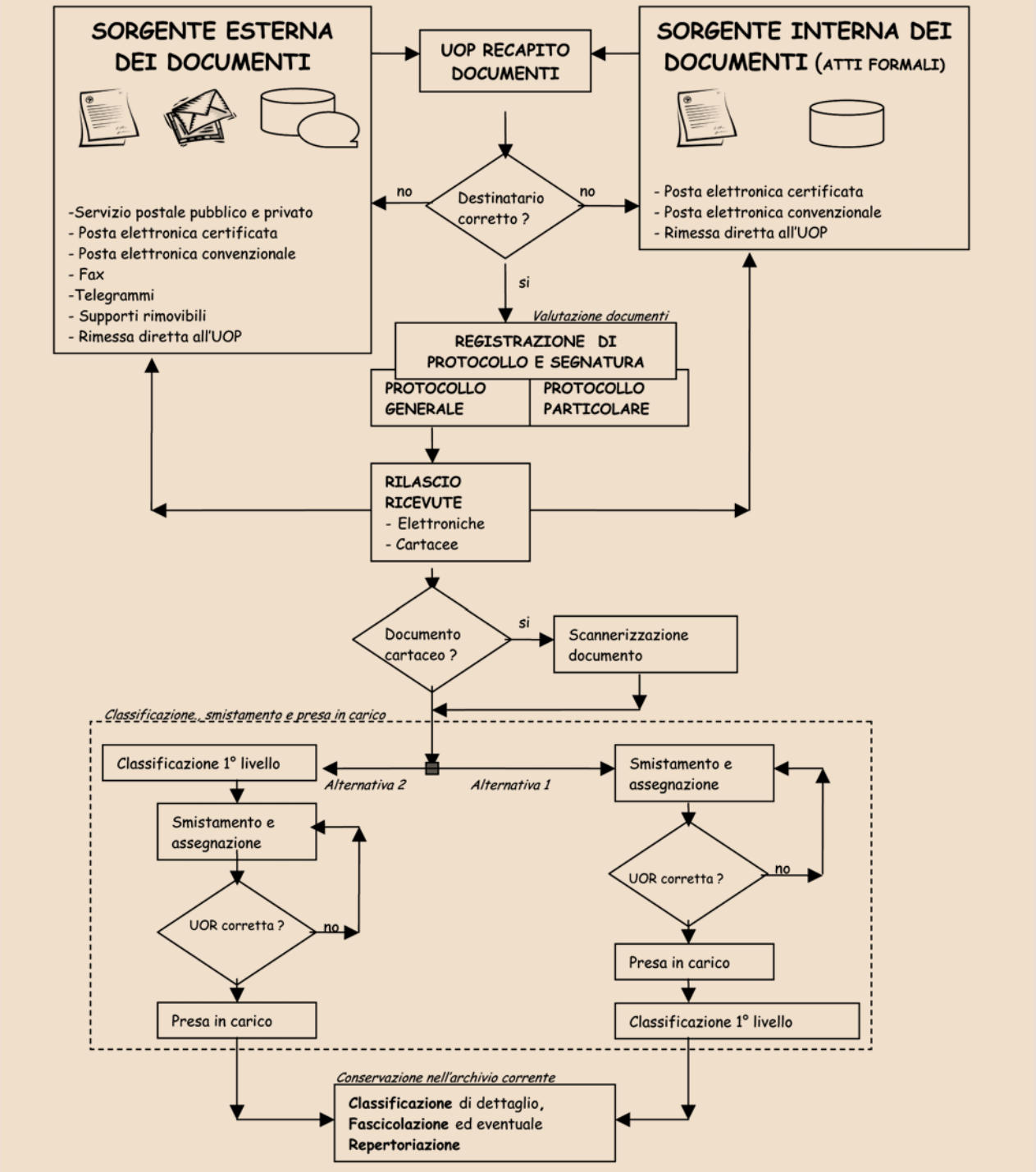
5.1 GENERALITÀ

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

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

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.
Come previsto dalla normativa vigente i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.
I flussi relativi alla gestione dei documenti all'interno dell'AOO sono descritti graficamente nel paragrafo seguente prendendo in esame quelli che possono avere rilevanza giuridico-probatoria.
Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.
I flussi dei documenti interni di tipo informale trasmessi e ricevuti vengono descritti nell'allegato *descrizione dei flussi dei documenti all'interno dell'AOO*.

5.2 FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO



5.2.1 PROVENIENZA ESTERNA DEI DOCUMENTI

I documenti che sono trasmessi da soggetti esterni all'amministrazione sono, oltre quelli richiamati nel capitolo precedente, i telefax, i telegrammi e i supporti digitali rimovibili. Questi documenti sono recapitati alla/e UOP designata/e.

I documenti che transitano attraverso il servizio postale sono ritirati quotidianamente secondo le regole stabilite dal RSP riportate nell'allegato *Regole di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale*.

5.2.2 PROVENIENZA DI DOCUMENTI INTERNI FORMALI

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

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

I mezzi di recapito della corrispondenza considerati sono la posta elettronica convenzionale o certificata.

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

5.2.3 RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ISTITUZIONALE

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

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

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

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

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

Il responsabile dello smistamento controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e verifica se sono da protocollare.

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

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

5.2.5 RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI RIMOVIBILI

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

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

5.2.6 RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE

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

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

Qualora una AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UOR aperta al pubblico, oltre, ovviamente alle UOP istituzionali, ovvero se per errore la corrispondenza viene recapitata ad un UOR quest'ultimo, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente nelle forme stabilite dal RSP, e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UOP abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.
Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.
In ogni caso i documenti così ricevuti devono essere inviati a cura dell'UOR/UU in busta chiusa, nella stessa giornata, prima della chiusura del servizio di protocollo, a una delle UOP autorizzata all'apertura della corrispondenza.

5.2.8 ERRATA RICEZIONE DI DOCUMENTI DIGITALI

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

5.2.9 ERRATA RICEZIONE DI DOCUMENTI CARTACEI

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

- busta indirizzata ad altra AOO della stessa amministrazione:
  a) si invia alla AOO corretta;
  b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore";
- busta indirizzata ad altra amministrazione:
  a) si restituisce alla posta;
  b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

5.2.10 ATTIVITÀ DI PROTOCOLLAZIONE DEI DOCUMENTI

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

5.2.11 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI INFORMATICI

La ricezione di documenti comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica.
Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.
Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

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

5.2.12 RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.
La semplice apposizione del timbro datario dell'UOP per la tenuta del protocollo sulla

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

- fotocopiare gratuitamente la prima pagina del documento;
- apporre 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 agli UU, attraverso la rete interna dell'amministrazione/AOO, subito dopo l'operazione di smistamento e di assegnazione.

5.2.14 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

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

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

Le rappresentazioni digitali dei documenti cartacei sono archiviate secondo le regole vigenti, in modo non modificabile al termine del processo di scansione.
I documenti cartacei dopo l'operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della delibera CNIPA 19 febbraio 2004 n.11 vengono inviati agli UOR/UU/RPA destinatari per le operazioni di fascicolazione e conservazione.
I documenti con più destinatari, sono riprodotti in formato immagine ed inviati solo in formato elettronico.
La riproduzione dei documenti cartacei in formato immagine viene eseguita sulla base dei seguenti criteri:

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

  – i certificati medici contenenti la diagnosi

  – certificati di invalidità

– certificati contenenti dati sensibili;

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 ad UU o direttamente al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione in essere presso l'amministrazione.

5.2.16 CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE

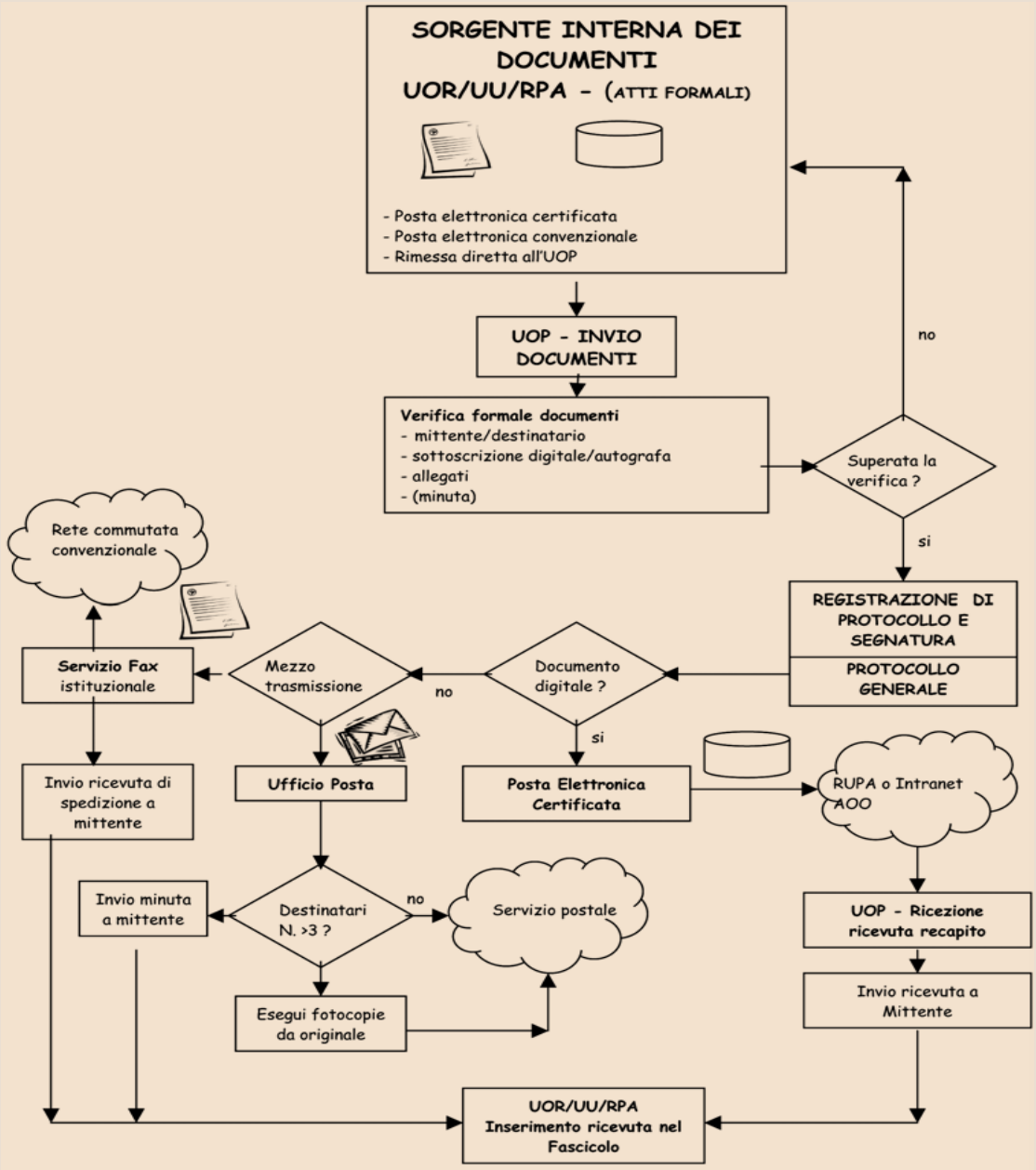
Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

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

5.2.17 CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI NELLA FASE CORRENTE

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

5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO



5.3.1 SORGENTE INTERNA DEI DOCUMENTI

Nel grafico di cui al paragrafo 5.3 per sorgente interna (all'AOO) dei documenti si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il RPA, la corrispondenza alla UOP della AOO stessa affinché sia trasmessa, nelle forme e nelle modalità più opportune, ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.

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

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

I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati

nell'articolo 35 Posta Elettronica Certificata.
Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.
I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.
Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo è il servizio postale.

5.3.2 VERIFICA FORMALE DEI DOCUMENTI

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

5.3.3 REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

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

5.3.4 TRASMISSIONE DI DOCUMENTI INFORMATICI

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AGID 23 gennaio 2013, n. 60.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).
Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dall'AGID.
Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.
Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti

formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

5.3.5 TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA

La UOR provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.

5.3.6 AFFRANCATURA DEI DOCUMENTI IN PARTENZA

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

5.3.7 CONTEGGI SPEDIZIONE CORRISPONDENZA

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

5.3.8 DOCUMENTI IN PARTENZA PER POSTA CONVENZIONALE CON PIÙ DESTINATARI

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

5.3.9 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:

L'attività di smistamento consiste nell'operazione di inviare un documento da protocollare e segnare all'UOR competente in base alla classificazione di primo livello del titolario, e/o all'oggetto del 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 e provvede alla registrazione del documento nel protocollo.

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 *area organizzativa omogena e modello organizzativo* sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.

Lo smistamento iniziale eseguito dalla/e UOP recapita ai dirigenti di ciascuna UOR, attraverso funzioni specifiche del sistema di protocollo informatico, i documenti indirizzati all'UOR medesimo.

Quest'ultimi, dopo averne preso visione, provvedono ad accettarli e ad assegnarli ai propri UU/RPA, oppure in caso di errore, ad informare il mittente (UOP) e a smistare la notifica ad altro UOR.

L'UOR del procedimento amministrativo indica, sul documento in arrivo, il nominativo del RPA. Qualora non sia diversamente specificato il RPA coincide con il dirigente dell'UOR.

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, 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 e smistamento.
Il responsabile dell'UOR può protocollare il documento, applicare la segnatura di protocollo, visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:

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

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

6.4 ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO

I documenti ricevuti dall'amministrazione in formato cartaceo, *se successivamente acquisiti in formato immagine con l'ausilio di scanner*, una volta concluse le operazioni di registrazione, di segnatura e di assegnazione, sono fatti pervenire al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione/AOO. L'originale cartaceo può essere successivamente trasmesso al RPA oppure essere conservato dalla UOP.

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 xxx ore dal momento in cui sono pervenuti, salvo che vi siano, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

6.5 MODIFICA DELLE ASSEGNAZIONI

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

assegnazione è attribuita al dirigente della UOR medesima o a persona da questi incaricata.
Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

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

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO

In base al modello organizzativo adottato dall'Amministrazione/AOO (si veda il par. 1.4 del presente MdG), nell'allegato *area organizzativa omogena e modello organizzativo* 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 denominato Aruba Posta Elettronica Certificata SPA 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 dott.ssa Agosti Maria.

Nei casi di vacanza, assenza o impedimento del responsabile del servizio archivistico, questo sarà sostituto da Rinaldi Maria Elena.

L'atto che istituisce il servizio e nomina il relativo responsabile è riportato nell'allegato *Nomina del responsabile del servizio archivistico*.

7.2. SERVIZIO DELLA CONSERVAZIONE SOSTITUTIVA 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;

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.

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

8.1 DOCUMENTI ESCLUSI

Sono esclusi dalla registrazione di protocollo, le tipologie di documenti riportati nell'allegato *elenco dei documenti esclusi dalla registrazione del protocollo*.
Sono inoltre esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

8.2 DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati in *elenco dei documenti soggetti a registrazione particolare* allegato al presente MdG.
Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.
Questi documenti costituiscono comunque delle serie di interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

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

9. Sistema di classificazione, fascicolazione e piano di conservazione

9.1 PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

9.1.1 GENERALITÀ

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

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

Il piano di conservazione, allegato al presente MdG, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'AOO nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio.

Il titolario e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione.

Spetta ai vertici dell'amministrazione medesima adottare il titolario e il piano di conservazione con atti formali.

9.1.2 MISURE DI PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI

Gli archivi e i singoli documenti degli enti pubblici non territoriali sono beni culturali inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

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

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della direzione generale per gli archivi.

Relativamente agli enti pubblici non statali l'autorizzazione per l'eventuale rimozione e/o trasferimento dell'archivio, è demandata, per delega della direzione generale degli archivi, alle sovrintendenze archivistiche.

Lo scarto dei documenti degli archivi delle amministrazioni/AOO statali è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza corrispondente alla provincia o delle commissioni di scarto istituite presso ogni ufficio con

competenza subprovinciale. Per gli enti pubblici non statali la competenza è delegata alla soprintendenza archivistica competente per territorio.
Per l'archiviazione e la custodia nella sezione di deposito o storica dei documenti contenenti dati personali, si applicano in ogni caso le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

9.2 TITOLARIO O PIANO DI CLASSIFICAZIONE

9.2.1 TITOLARIO

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.
Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc.
Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato *Titolario di classificazione*.
Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo dell'amministrazione.
Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali.
L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP (oppure, su proposta del responsabile dell'archivio generale dell'amministrazione e/o dalle autorità competenti per materia).
La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno.
Dopo ogni modifica del titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti.
Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.
Per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione.
Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo titolario e valgono almeno per l'intero anno.
Rimane possibile, se il sistema lo consente, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.
Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

9.2.2 CLASSIFICAZIONE DEI DOCUMENTI

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

9.3 FASCICOLI E DOSSIER

9.3.1 FASCICOLAZIONE DEI DOCUMENTI

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.
I documenti sono archiviati all'interno di ciascun fascicolo o inserto, secondo l'ordine cronologico di registrazione.

9.3.2 APERTURA DEL FASCICOLO

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'ente, il soggetto preposto (quale, ad esempio, RPA, RSP, responsabile del servizio archivistico addetto alla protocollazione, etc.) provvede all'apertura di un nuovo fascicolo.
La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione, (cioè titolo, classe, sottoclasse, etc.);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'amministrazione;
- data di apertura del fascicolo;
- UOR;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario.

9.3.3 CHIUSURA DEL FASCICOLO

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare.
La data di chiusura si riferisce alla data dell'ultimo documento prodotto.
Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo 9.3.2, primo capoverso, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

9.3.4 PROCESSO DI ASSEGNAZIONE DEI FASCICOLI

Quando un nuovo documento viene recapitato all'amministrazione, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce a un nuovo affare o procedimento per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- Se il documento si ricollega ad un *affare o procedimento in corso*, l'addetto:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato;
  - invia il documento all'UOR cui è assegnata la pratica.
- Se il documento dà avvio ad un *nuovo fascicolo*, il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo;
  - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
  - assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
  - invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

9.3.5 MODIFICA DELLE ASSEGNAZIONI DEI FASCICOLI

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.

Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore di UU che effettua la modifica con la data e l'ora dell'operazione.

9.3.6 REPERTORIO DEI FASCICOLI

I fascicoli sono annotati nel repertorio dei fascicoli.

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

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

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

Nel repertorio sono indicati:

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

inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

9.3.7 APERTURA DEL DOSSIER

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

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

9.3.8 REPERTORIO DEI DOSSIER

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

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

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

Il repertorio dei dossier è costantemente aggiornato.

9.4 SERIE ARCHIVISTICHE E REPERTORI

9.4.1 SERIE ARCHIVISTICHE

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

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

I fascicoli subiscono il processo di selezione e scarto dei documenti; le serie così composte, faranno parte, successivamente, della sezione storica dell'archivio.

9.4.2 REPERTORI E SERIE ARCHIVISTICHE

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

Ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

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

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.
Il repertorio è costantemente aggiornato.

9.4.3 VERSAMENTO DEI FASCICOLI NELL'ARCHIVIO DI DEPOSITO

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

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;

Il RPA/UU provvede inoltre:

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

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

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

L'ufficio ricevente esegue il controllo del materiale riversato.
Il servizio archivistico dell'amministrazione/AOO riceve agli atti soltanto i fascicoli con materiale ordinato e completo.
Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito agli UOR/UU tenutari dell'archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie.

Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, il responsabile degli UOR deposita il fascicolo dichiarando ufficialmente che è incompleto e si assume la responsabilità della trasmissione agli atti.
Ricevuti i fascicoli e controllato il relativo elenco, il responsabile del servizio archivistico dell'amministrazione firma per ricevuta l'elenco di consistenza.

9.5 SCARTO, SELEZIONE E RIORDINO DEI DOCUMENTI

9.5.1 OPERAZIONE DI SCARTO

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.
Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.
La legge impone all'amministrazione/AOO l'uso o la predisposizione di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio.

In caso di predisposizione ex novo, il massimario viene proposto dal RSP (**opzionale** coadiuvato dal responsabile dell'archivio generale), alla direzione generale degli archivi del Ministero per i beni e le attività culturali e viene autorizzato con atto formale dall'organo competente dell'amministrazione.
Le operazioni di selezione e scarto sono effettuate, sotto la vigilanza del RSP (o da persona delegata, ad esempio il responsabile dell'archivio), a cura degli addetti del servizio archivistico.

9.5.2 CONSERVAZIONE DEL MATERIALE PRESSO LA SEZIONE DI DEPOSITO DELL'ARCHIVIO

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

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

9.6.1 PRINCIPI GENERALI

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

9.6.2 CONSULTAZIONE AI FINI GIURIDICO-AMMINISTRATIVI[5]

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15 che qui di seguito si riporta.

"1. Il diritto di accesso è escluso:
a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive

modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
a) quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con
particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si
riferiscono;
e) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.
7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in
caso di dati idonei a rivelare lo stato di salute e la vita sessuale).”

9.6.3 CONSULTAZIONE PER SCOPI STORICI

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata dal regolamento emanato da ciascuna amministrazione.
La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell’interno (a norma dell’art. 125 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione/AOO. È possibile l’ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell’interno, su conforme parere dell’autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);

- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto
- consultatore.

9.6.4 CONSULTAZIONE DA PARTE DI PERSONALE ESTERNO ALL'AMMINISTRAZIONE

La domanda di accesso ai documenti viene presentata al servizio archivistico o all'Ufficio
Relazioni con il Pubblico (URP), che provvede a smistarla al servizio archivistico.
Presso il servizio archivistico e l'URP sono disponibili appositi moduli come quelli riportati nell'allegato *modulo di consultazione della sezione di deposito e storica dell'archivio.*
Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla soprintendenza per i beni archivistici territorialmente competente, con apposito modulo da questa predisposto.
Le domande vengono evase durante gli orari di apertura al pubblico dell'URP e dell'archivio con la massima tempestività e comunque non oltre 20 giorni lavorativi dalla presentazione.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.
In tale caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.
In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.
L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico.
La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.
Il rilascio di copie dei documenti dell'archivio avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.
In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.
Le disposizioni dei commi precedenti si applicano anche alla consultazione di archivi storici presso le pubbliche amministrazioni che non si siano ancora dotate di apposito servizio per l'apertura alla pubblica consultazione degli archivi.

9.6.5 CONSULTAZIONE DA PARTE DI PERSONALE INTERNO ALL'AMMINISTRAZIONE

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica.
L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio del medesimo UOR/UU od altro UOR/UU avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.
Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo

avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.
Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.
Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.
Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo.
Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'amministrazione/AOO.
In ogni caso deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

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

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

10.1 UNICITÀ DEL PROTOCOLLO INFORMATICO

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

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

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

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

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

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

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

Non è consentita la protocollazione di un documento già protocollato.

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

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

10.2 REGISTRO GIORNALIERO DI PROTOCOLLO

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è inviato in Conservazione Sostitutiva, ai sensi del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, art 7 c5, anche tramite gli automatismi del PdP.

Tale operazione di riversamento viene espletata all'interno del PdP.

È a carico del Conservatore conservare in modalità sicura la copia del registro giornaliero di protocollo.

10.3 REGISTRAZIONE DI PROTOCOLLO

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali,

digitali o informatici e analogici).
Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.
Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

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

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

10.3.1 DOCUMENTI INFORMATICI

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'amministrazione.
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.
Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

10.3.2 DOCUMENTI ANALOGICI (CARTACEI E SUPPORTI RIMOVIBILI)

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

10.4 ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO

Il RSP, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del

protocollo.
La registrazione degli elementi facoltativi del protocollo, con determinazione del RSP può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.
Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

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

10.5 SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
Essa consente di individuare ciascun documento in modo inequivocabile.

10.5.1 DOCUMENTI INFORMATICI

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

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;

- data e numero di protocollo del documento.

È facoltativo riportare anche le seguenti informazioni:

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

Per i documenti informatici in partenza, possono essere specificate, in via facoltativa, anche le seguenti informazioni:

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

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

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

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

Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal AGID (circolare AGID del 23 gennaio 2013, n 60).

10.5.2 DOCUMENTI CARTACEI

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

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

Facoltativamente possono essere riportate anche le seguenti informazioni:

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

L'operazione di segnatura dei documenti in partenza viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dalla UOP.

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

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

10.6 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare anche un solo campo *tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile* per correggere errori verificatisi in sede di immissione manuale di dati o attraverso

l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.
L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.
A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.
Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

10.7 LIVELLO DI RISERVATEZZA

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

10.8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

10.8.1 REGISTRAZIONI DI PROTOCOLLO PARTICOLARI (RISERVATE)

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

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

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

- se ritiene che contengano dati o informazioni di interesse dell'amministrazione/AOO,

provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni. Questi decidono se registrarli, farli registrare nel protocollo generale;

- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo riservato.

10.8.2 CIRCOLARI E DISPOSIZIONI GENERALI

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

10.8.3 DOCUMENTI CARTACEI IN PARTENZA CON PIÙ DESTINATARI

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale (se cartaceo) con la dicitura "Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari Vedi elenco allegato alla minuta/copia presso l'UOR/UU/RPA".
Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

10.8.4 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEGRAMMA

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

10.8.5 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX

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

> *"In linea generale i fax gestiti con i servizi di invio e ricezione tramite l'utilizzo della rete internet si ritiene assumano valore equivalente a quello dei fax tradizionali, rientrando la fattispecie nella disposizione di cui all'articolo 38 del DPR 445/2000. Tuttavia, le specifiche modalità di validità delle istanze e delle dichiarazioni presentate alla P.A., previste dall'articolo 65 del CAD, sottendono la necessità di identificare il soggetto che presenta l'istanza o la dichiarazione.*
>
> *Tali modalità non sono presenti nel servizio di netfax in quanto esso consente di individuare una singola utenza telefonica, ma non specificamente colui che presenta l'istanza o la dichiarazione."*
>
> *Risposta AGID sulla validità del messaggio giunto via telefax.*

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".

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

10.8.6 PROTOCOLLAZIONE DI UN NUMERO CONSISTENTE DI DOCUMENTI CARTACEI

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

10.8.7 DOMANDE DI PARTECIPAZIONE A CONCORSI, AVVISI, SELEZIONI, CORSI E BORSE DI STUDIO

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.
Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.
Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

10.8.8 FATTURE, ASSEGNI E ALTRI VALORI DI DEBITO O CREDITO

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall'altra posta in arrivo, protocollate su un registro diverso da quello generale e inviate quotidianamente all'UOR competente.

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

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

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

10.8.10 PROTOCOLLI URGENTI

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

10.8.11 DOCUMENTI NON FIRMATI

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

10.8.12 PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:
In caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;

- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

10.8.13 PROTOCOLLO DI DOCUMENTI DIGITALI PERVENUTI ERRONEAMENTE

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

10.8.14 RICEZIONE DI DOCUMENTI CARTACEI PERVENUTI ERRONEAMENTE

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

10.8.15 COPIE PER CONOSCENZA

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

10.8.16 DIFFERIMENTO DELLE REGISTRAZIONI

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

Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

10.8.17 REGISTRAZIONI DI DOCUMENTI TEMPORANEAMENTE RISERVATI

Quando si è in presenza di documenti che per la loro natura richiedono una temporanea riservatezza delle informazioni in essi contenute (ad esempio gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso riservato al protocollo generale.
Il responsabile dell'immissione dei dati provvede alla registrazione di protocollo indicando contestualmente l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate saranno accessibili nelle forme ordinarie.

10.8.18 CORRISPONDENZA PERSONALE O RISERVATA

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

10.8.19 INTEGRAZIONI DOCUMENTARIE

Il Responsabile del Procedimento Amministrativo (RPA) è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta e, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

10.9 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL PDP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di

registrazione, il versamento dei documenti in conservazione, sono effettuate attraverso il PdP.
Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

10.10 REGISTRAZIONI DI PROTOCOLLO

10.10.1 ATTRIBUZIONE DEL PROTOCOLLO

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

10.10.2 REGISTRO INFORMATICO DI PROTOCOLLO

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

- estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di protocollo;
- invio alla conservazione sostitutiva del registro.

L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

11. Descrizione funzionale ed operativa del sistema di protocollo informatico

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

11.1 DESCRIZIONE FUNZIONALE ED OPERATIVA

Di seguito viene fornita una elencazione sintetica delle principali funzioni del PdP.
Non viene trattato delle modalità operative perché quest'ultime sono trattate dettagliatamente nel Manuale utente del PdP.
Il Pdp permette:

1. La creazione e la profilazione degli utenti, permettendo in maniera capillare permettendone in maniera univoca l'identificazione (DPCM 3 dicembre 2013 art 7 c. 1)
2. L'accesso alle risorse solo agli utenti abilitati, permettendo la visualizzazione dei soli documenti permessi. (DPCM 3 dicembre 2013 art 7 c. 2)
3. La registrazione delle attività svolte da ciascun utente (DPCM 3 dicembre 2013 art 7 c. 3)
4. La trasmissione del registro protocollo giornaliero al conservatore scelto dall'amministrazione (DPCM 3 dicembre 2013 art 7 c. 5)
5. La registrazione dei documenti e l'assegnazione degli stessi agli UU
6. La ricerca dei documenti in maniera rapida
7. La creazione e la collazione dei documenti in pratiche, cartelle e fascicoli
8. La repertoriazione dei documenti
9. La possibilità di acquisire in maniera automatica le comunicazioni giunte attraverso le caselle di posta certificata istituzionale e le caselle di posta elettronica ordinarie in uso all'amministrazione
10. La possibilità di inviare ricevute elettroniche dei documenti ricevuti
11. Il controllo assiduo delle operazioni svolte
12. La possibilità di assegnare documenti tra le UOR

12. Rilascio delle abilitazioni di accesso alle informazioni documentali

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

12.1 GENERALITÀ

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

- una credenziale di accesso, costituita, ad esempio, da una componente:
  - pubblica che permette l'identificazione dell'utente da parte del sistema (*userID*);
  - privata o riservata di autenticazione (*password*);
- una autorizzazione di accesso all'UOR 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.
- una autorizzazione di accesso al registro protocollo 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 4 profili d'accesso, sulla base delle rispettive competenze.

- *AMMINISTRATORE DEL PROTOCOLLO*
- *UTENTE PROTOCOLLANTE*
- *UTENTE PROTOCOLLANTE SOLO USCITA*
- *VISITATORE*

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

12.2 ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO

Gli utenti abilitati accedono al PdP accedendo al portale unico di accesso e inseriscono le proprie credenziali di riconoscimento.

In base al profilo di accesso vengono mostrate loro le attività possibili e gli elenchi di documenti

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.
Le password sono salvate in modo crittografato e non è possibile risalire alla password in dotazione dell'utente.
Tutte le utenze dell'AOO sono configurate con un *time-out* che provvede a disconnettere automaticamente l'applicazione dopo 120 minuti di inattività.
Le sessioni multiple con la stessa *user ID* sono proibite e impedite dal PdP.

12.3 PROFILI DI ACCESSO

12.3.1 Utente amministratore di PDP

L'utente amministratore di PdP ha i privilegi massimi di sicurezza, può gestire e controllare le anagrafiche, assegnare ruoli e permessi agli altri utenti, ha l'accesso a tutte le UOR e può visualizzare tutti i documenti.
Può gestire fascicoli e dossier, il titolario di classificazione e le specifiche del registro.

12.3.2 Utente protocollante

L' "utente protocollante" ha la gestione dei documenti secondo l'abitazione assegnata, può protocollare, inserire in fascicoli e dossier.

12.3.3 UTENTE protocollante solo uscita

L' "utente protocollante solo uscita" ha la gestione dei documenti cui gli è stato dato accesso, può protocollare, inserire in fascicoli e dossier. Le sue azioni di protocollazione, tuttavia, sono limitate solo ai documenti in uscita.

12.3.4 Utente Visitatore

Il profilo "visitatore" ha l'accesso alla visualizzazione dei documenti inseriti in un UOR e può visualizzare o stampare i documenti cui gli è stato dato accesso.

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

Al fine di procedere alla creazione delle utenze il RSP – accreditatosi con le credenziali di riconoscimento - entra nell'area del PdP preposta alla creazione dell'utente e inizia l'attività di profilamento assegnando un profilo di lavoro per ciascuna UOR in cui l'UU avrà accesso, scegliendo tra i profili a disposizione.
Allo stesso modo l'UU viene profilato per l'accesso al registro, stabilendo il profilo adeguato alla sicurezza dell'utente. Consegna quindi le credenziali all'UU.

12.5 RIPRISTINO DELLE CREDENZIALI PRIVATE D'ACCESSO

Nel caso in cui l'UU abbia dimenticato le password d'accesso il RSP può impostare una password temporanea che l'UU potrà modificare al primo accesso.

13. Modalità di utilizzo del registro di emergenza

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

13.1 IL REGISTRO DI EMERGENZA

Qualora non fosse disponibile fruire del PdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

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

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

Il registro di emergenza si configura come un repertorio del protocollo generale.

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

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

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

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

13.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

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

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

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

L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nel documento *area organizzativa omogena e modello organizzativo*, allegato al presente MdG.

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

13.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

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

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

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

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

13.4 MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA

È compito del RSP verificare la chiusura del registro di emergenza.

È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.

Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

Per semplificare la procedura di chiusura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) analogo a quello utilizzato nella fase di apertura del registro di emergenza.

14. Gestione dei procedimenti amministrativi

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

14.1 MATRICE DELLE CORRELAZIONI

I procedimenti amministrativi sono descritti nel "Catalogo dei procedimenti amministrativi", di cui il RSP cura l'aggiornamento, estemporaneo o periodico.
I procedimenti amministrativi costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'amministrazione/AOO.
All'interno del catalogo i procedimenti sono individuati mediante la definizione dei riferimenti riportati al successivo paragrafo 14.2.
La definizione del singolo procedimento amministrativo rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.
Il risultato concreto di questa attività sono i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare.
L'individuazione del RPA e del responsabile dell'adozione del provvedimento finale è effettuata sulla base delle competenze assegnate a ciascuna figura interna agli UOR/UU.

14.2 CATALOGO DEI PROCEDIMENTI AMMINISTRATIVI

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

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

14.3 AVVIO DEI PROCEDIMENTI E GESTIONE DEGLI STATI DI AVANZAMENTO

Mediante l'assegnazione dei fascicoli agli UOR/UU di volta in volta competenti, le UOP o i RPA provvedono a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente.
La registrazione degli stati di avanzamento dei procedimenti amministrativi sulla base informativa sopra richiamata può avvenire in modalità manuale o automatica.

Nel primo caso, gli stati di avanzamento sono aggiornati dal RPA.
Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

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

15.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

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

Il presente Manuale potrà essere aggiornato a seguito di:

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

15.2 REGOLAMENTI ABROGATI

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

15.3 PUBBLICITÀ DEL PRESENTE MANUALE

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

- fornita a tutto il personale dell'AOO e se possibile resa disponibile mediante la rete intranet;
- pubblicata sul sito internet dell'amministrazione.

15.4 OPERATIVITÀ DEL PRESENTE MANUALE

Il presente regolamento è operativo una volta approvato.

Allegato 1 (elenco dei documenti esclusi dalla registrazione di protocollo)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

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

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)
- convocazioni ad incontri o riunioni e corsi di formazione interni
- delibere, disposizioni interne, ordini di servizio e comunicazioni al personale
- modulistica attinente a ferie, missioni, fornitura di materiali ed equipaggiamenti informatici, rapporti valutativi e documentazione simile
- atti notificati a mano ai dipendenti
- ricevute di ritorno delle raccomandate A.R

Allegato 2 (elenco dei documenti soggetti a registrazione particolare)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

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

L'ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE PER TUTTE LE AMMINISTRAZIONI E' IL SEGUENTE:

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

Allegato 3 (massimario di scarto)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

TIPO DI DOCUMENTO	Illimitata	almeno 10 anni	almeno 6 anni	almeno 1 anno	Campione un anno ogni 10
1. Circolari interne e ordini di servizio	X				
2. Bilanci Preventivi e Consuntivi	X				
3. Documenti contabili (esclusi quelli di cui al n.2)		X			X*
4. Verbali commissioni elettorali degli organi collegiali	X				
5. Documenti prodotti per l'elezione di organi collegiali (esclusi quelli di cui al n.4)			X		
6. Elaborati delle prove scritte, grafiche e pratiche (esclusi quelli prodotti per gli esami di Stato)				X	X*
7. Elaborati delle prove scritte, grafiche e pratiche prodotti per gli esami di Stato	X				
8. Domande di supplenza del personale docente ed ATA				X	
9. Libretto di macchina (con consumo di carburante)			X		
10. Registri Inventariali	X				
11. Registri di protocollo (o registri della posta in arrivo e in partenza)	X				
12. Registri delle assenze del personale docente ed ATA			X		
13. Registro dei certificati di studio e di servizio rilasciati			X		
14. Registro delle autorizzazioni ad impartire lezioni private			X		
15. Registro della corrispondenza recapitata a mano			X		
16. Registro di magazzino			X		
17. Registro delle raccomandate			X		
18. Registro delle tasse scolastiche			X		
19. Registri dei verbali delle deliberazioni degli organi collegiali	X				
20. Registro del telefono				X	
21. Tabelle di liquidazione delle competenze			X		
22. Verbali dei passaggi di consegne	X				
23. Libretti scolastici non consegnati agli alunni			X		
24. Registri delle assenze degli			X		

alunni					
25. Registri di classe (giornali di classe)	X				
26. Registri di iscrizione degli alunni	X				
27. Registri di carico e scarico dei diplomi degli allievi	X				
28. Registri di consegna dei diplomi	X				
29. Registri dei verbali degli esami	X				
30. Documenti prodotti dagli alunni e dai candidati per l'iscrizione e l'ammissione agli esami, ad eccezione del titolo di studio originale (da restituire all'interessato) N.B. il calcolo degli anni decorre dalla cessazione della appartenenza all'Istituto o dall'iscrizione agli esami			X		

Allegato 4 (modulo di consultazione della sezione di deposito e storica dell'archivio)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

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

Spett.le Dirigente Scolastico
RC GIOVANNI FALCONE

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

Scopo della consultazione:
.....
.....

Durata indicativa della consultazione: ..... mesi

Materiale da consultare:

o **Titolo** .....
o **Classe** .....
o **Sottoclasse** .....

o **Descrizione dei fascicoli:**

• Oggetto del fascicolo: .....
• Anno di repertoriazione .....
• Dal numero ..... al numero .....

o **Descrizione dei sottofascicoli:**

• Oggetto del fascicolo: .....
• Anno di repertoriazione .....
• Dal numero ..... al numero .....

o **Descrizione degli inserti:**

• Oggetto del fascicolo: .....
• Anno di repertoriazione .....
• Dal numero ..... al numero .....

NOTE: .....
.....

Data, ...

L'OPERATORE RICEVENTE: .....

IL RESPONSABILE DELL'ARCHIVIO: .....

Allegato 5 (nomina del responsabile della conservazione sostitutiva)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE SOSTITUTIVA

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

L'anno 2016, il giorno 22 del mese di g i u g n o, nell'amministrazione RC GIOVANNI FALCONE sita in PALAZZOLO SULL'OGLIO VIA LEVADELLO

IL DIRIGENTE

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

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

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

VISTA la determinazione del 22.06.2016 relativa alla nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;

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

RITENUTO di individuare nel/nella signor/signora Prof. Luciano Tonidandel, in carico presso questa Istituzione Scolastica la figura professionale più idonea ad espletare i compiti di seguito indicati:

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

DETERMINA

- di individuare il responsabile della conservazione dei documenti informatici il\la signor\a Prof. Luciano Tonidandel
- di individuare nel direttore dei servizi generali e amministrativi il funzionario tenuto alla vigilanza sugli adempimenti connessi alla gestione documentale e agli archivi per quanto compreso nei compiti connessi al profilo di appartenenza
- di rendere il presente decreto immediatamente esecutivo.

Il Dirigente Scolastico
(Prof. Luciano Tonidandel)

Allegato 6 (atto di nomina del responsabile del servizio per la tenuta del protocollo informatico della gestione dei flussi documentali e degli archivi)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

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

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

L'anno 2016, il giorno 22 del mese di giugno, nell'amministrazione RC GIOVANNI FALCONE sita in PALAZZOLO SULL'OGLIO - VIA LEVADELLO

IL DIRIGENTE

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

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

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

RITENUTO di individuare nel/nella signor/signora dott.ssa Agosti Maria, DSGA presso questo Istituto, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale anche su Internet;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il:
  - Responsabile dei sistemi informativi automatizzati,
  - Referente della pianificazione delle attività,
  - Responsabile della sicurezza dei dati personali, se nominato, o direttamente con il Titolare dei trattamenti dei dati di cui al d. lgs. 196/03,

- Responsabile del servizio archivistico,
- Responsabile della conservazione sostitutiva;

- attribuire il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;
- curare, anche attraverso altri responsabili, le funzionalità del sistema di gestione informatica del protocollo e della gestione documentale affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conservare le copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso esterno o da altre Amministrazioni e le attività di gestione degli archivi, quali, trasferimento dei documenti all'archivio di deposito, disposizioni per la conservazione degli archivi e Archivi storici;
- autorizzare le operazioni di annullamento della registratura di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme correnti da parte del personale autorizzato e degli incaricati.

DETERMINA

1. di nominare il/la signore/a dott.ssa Agosti Maria quale Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 comma 2 del DPR n. 445/2000 con i compiti specificati nelle premesse.

2. di nominare vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile, viene nominato il/la signor/signora Rinaldi Maria Elena.

Il Dirigente Scolastico
(Prof. Luciano Tonidandel)

Allegato 7 (piano formativo per il personale ATA)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

PIANO FORMATIVO PER IL PERSONALE

Esempio di pianificazione della formazione
o **Alternativa 1**
Amministrazione IIS Falcone di Palazzolo s/O BS

PER IL PERSONALE DELL'IIS FALCONE DI PALAZZOLO SULL'OGLIO I PIANI FORMATIVI PREVISTI SONO QUELLI INDICATI NELLE CIRCOLARI DI INIZIO ANNO RELATIVE ALL'ORGANIZZAZIONE DEL LAVORO PER IL PERSONALE ATA E NELLE DELIBERE DEL C.D. O PREVISTE DALL'ANIMATORE DIGITALE PER QUANTO RIGUARDA IL PERSONALE DOCENTE.

Allegato 8 (politiche di sicurezza)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

POLITICHE DI SICUREZZA

16.9.1 Politiche accettabili di uso del sistema informatico

16.9.1.1 Premessa

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

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

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

16.9.1.2 Scopo

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

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

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

16.9.1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...).

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

16.9.1.4 Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.

2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di

linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

16.9.1.5 Politiche Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in *stand-by* con un comando specifico.

4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.

5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.

7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.

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

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

16.9.2 Politiche Antivirus

16.9.2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.
I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.
I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

16.9.2.2 Scopo

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

16.9.2.3 Ambito di applicazione

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

16.9.2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di

archiviazione rimovibili, usare questo protetto in scrittura.

- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.
- Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.
- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

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

16.9.2.5 Politiche per le azioni consuntive

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

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

16.9.3 Politiche Uso non accettabile

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).
2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
3. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

16.9.3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
   a) accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
   b) attività di "sniffing";
   c) disturbo della trasmissione;
   d) spoofing dei pacchetti;
   e) negazione del servizio;
   f) le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
   g) attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle

applicazioni.

12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

16.9.3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

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

16.9.4 Linee telefoniche commutate (analogiche e digitali)

16.9.4.1 Scopo

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

16.9.4.2 Ambito di applicazione

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

16.9.4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.
3. Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da

tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

16.9.4.4 Politiche – Telefax

Dovrebbero essere adottate le seguenti regole:

- le linee fax dovrebbero essere approvate solo per uso istituzionale;
- nessuna linea dei telefax dovrebbe essere usata per uso personale;
- Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
- Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

16.9.4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.
2. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

16.9.4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

16.9.5 Politiche per l'inoltro automatico di messaggi di posta elettronica

16.9.5.1 Scopo

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

16.9.5.2 Ambito di applicazione

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

16.9.5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi

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

16.9.6 Politiche per le connessioni in ingresso su rete commutata

16.9.6.1 Scopo

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

16.9.6.2 Ambito di applicazione

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

16.9.6.3 Politiche

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

16.9.7 Politiche per l'uso della posta istituzionale dell'amministrazione

16.9.7.1 Scopo

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

16.9.7.2 Ambito di applicazione

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

16.9.7.3 Politiche – Usi proibiti

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

16.9.7.4 Politiche – Uso personale

1. È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:
   a. i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
   b. venga utilizzata una ragionevole quantità di risorse pubbliche;
   c. non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
3. L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.
4. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

16.9.8 POLITICHE PER LE COMUNICAZIONI WIRELESS

16.9.8.1 Scopo

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

16.9.8.2 Ambito di applicazione

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

16.9.8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli

(auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

16.9.8.4 Politiche – Approvazione delle tecnologie

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

Allegato 9 (regola di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

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

1. La corrispondenza viene quotidianamente consegnata dall'Ufficio Postale entro le ore 13.00 di ogni giorno;
2. La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, ecc… viene consegnata in busta chiusa al servizio postale pubblico entro le ore 13,00 di ogni giorno;
3. Gli Uffici Utente devono far pervenire la posta in partenza all'Ufficio Posta della UOP generale che esegue la spedizione, entro e non oltre le ore 11:00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

Allegato 10 (Normativa di riferimento)

al Manuale di Gestione
Del Protocollo Informatico

Art. 5 DPMC 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario

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).
29. *L. 28 gennaio 2009, n. 2* Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (estratto relativo alla PEC)
29. *DPCM 30 marzo 2009* Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
30. *L. 18 giugno 2009, n. 69* Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile (estratto relativo all'Amministrazione digitale)
29. *DECRETO LEGISLATIVO 30 dicembre 2010*, n. 235 Modifiche ed integrazioni al decreto legislativo 7 Marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. (11G0002) (GU n.6 del 10-1-2011 - Suppl. Ordinario n. 8)
30. *DPCM 22 luglio 2011* Comunicazioni Imprese PA
31. *Circolare AGID del 23 gennaio 2013, n 60* Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni.
32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario;
32. *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 59

del 12 marzo 2014 - supplemento ordinario;

33. *Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014* - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015;

Allegato 11 (registro di emergenza)

Ministero dell'Istruzione, dell'Università e della Ricerca

RC GIOVANNI FALCONE

Scheda di apertura/chiusura del registro di emergenza

Causa dell'interruzione: _____

Data inizio evento: ___/____/_____ ___:____ Data fine evento: ___/____/_____ ___:____

Annotazioni: _____

Numero protocollo: iniziale _____ finale _____ Pagina n._____

DATA REGISTR.	Numero	DIR. (E/U)	TITOLARIO	MITTENTE / DESTINATARIO	OGGETTO

DATA REGISTR.	Numero	DIR. (E/U)	TITOLARIO	MITTENTE / DESTINATARIO	OGGETTO

DATA REGISTR.	Numero	DIR. (E/U)	TITOLARIO	MITTENTE / DESTINATARIO	OGGETTO

Il Responsabile del servizio Protocollo
dott.ssa Agosti Maria