

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

PER



Ministero dello
Sviluppo Economico

Nome del progetto:	"Manuale di Gestione del Protocollo Informatico"		
Data:	16/6/2016	Versione:	1.6.1
Autore:	Marco Monaci (Business-e S.p.A.); Antonio Maria Tambato (MISE)		
Nome documento:	Mise_manuale_gestione_protocollo_informativo_v1.6.1.docx		
Classificazione:	Pubblico		

VERSIONE DEL DOCUMENTO

Revisione	Revisione precedente	Sintesi dei cambiamenti	Changes Marked
1.6	-	Publicazione	-
1.6.1		Pubblicazione sito internet MISE	

DISTRIBUZIONE

Questo documento è distribuito a:

Nome	Titolo	Data	Versione
Sito intranet MISE			1.6
Sito internet MISE			1.6.1

INDICE DEL DOCUMENTO

1. PRINCIPI GENERALI	9
1.1 Premessa.....	9
1.2 Ambito di applicazione del Manuale	10
1.3 Definizioni e acronimi	10
1.4 Norme di riferimento	11
1.5 Aree Organizzative omogenee e modelli organizzativi	12
1.6 Servizio per la gestione informatica del protocollo	13
1.7 Tutela dei dati personali.....	14
1.8 Caselle di posta elettronica.....	15
1.9 Accreditamento dell'amministrazione all'IPA	15
1.10 Formazione	16
2. PIANO DI SICUREZZA	18
2.1 Obiettivi del piano di sicurezza	18
2.2 Generalità.....	18
2.3 Formazione dei documenti - Aspetti di sicurezza	20
2.4 Gestione dei documenti informatici	21
2.5 Trasmissione e interscambio dei documenti informatici.....	21
2.6 Accesso ai documenti informatici.....	22
2.7 Conservazione dei documenti informatici	23
3. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI	24
3.1 Il documento informatico	24
3.2 Il documento analogico - cartaceo	25
3.3 Formazione dei documenti - aspetti operativi.....	25
3.4 Requisiti degli strumenti informatici di scambio	26
3.5 Firma digitale.....	27
3.5.1 Tipi di firma digitale.....	27
3.5.2 Dispositivi che contengono i certificati di firma	28
3.5.3 Generazione dei documenti pdf e pdf ricercabili	28
3.5.4 Marcatura temporale	29

3.5.5	Documenti informatici e protocollazione	29
3.5.6	Copie e trasmissione di documenti informatici	29
3.5.7	Gli strumenti forniti dal MISE	30
3.6	<i>Verifica delle firme con il PdP</i>	31
3.7	<i>Uso della Posta Elettronica Certificata</i>	31
4.	DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI	34
4.1	<i>Generalità</i>	34
4.2	<i>Procedura per la protocollazione dei messaggi di Posta Elettronica Certificata (PEC)</i>	35
4.3	<i>Flussi procedurali per la protocollazione delle PEC</i>	36
4.3.1	PEC in entrata	36
4.3.2	PEC in uscita.....	37
4.4	<i>Flussi procedurali per la protocollazione dei documenti cartacei</i>	39
4.4.1	Protocollazione in entrata	39
4.4.2	Protocollazione in uscita o interna	41
4.5	<i>Procedura Flusso UCB</i>	43
4.6	<i>Procedure di gestione di flussi documentali specifiche delle Direzioni Generali</i>	43
5.	ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	44
5.1	<i>Documenti esclusi</i>	44
5.2	<i>Documenti soggetti a registrazione particolare</i>	44
6.	IL SISTEMA DI CLASSIFICAZIONE.....	45
6.1	<i>Protezione e conservazione degli archivi pubblici</i>	45
6.1.1	Generalità	45
6.1.2	Misure di protezione e conservazione degli archivi pubblici.....	45
6.2	<i>Classificazione dei documenti, Titolare e Piano di conservazione</i>	45
6.2.1	Titolario	46
6.2.2	Piano di conservazione	46
6.3	<i>Scarto, selezione e riordino dei documenti</i>	47
6.3.1	Operazione di scarto.....	47
6.3.2	Conservazione del materiale presso la sezione di deposito dell'archivio	47
6.3.3	Versamento dei documenti nell'archivio storico.....	48
6.4	<i>Consultazione e movimentazione dell'archivio corrente, di deposito e storico</i>	48

6.4.1	Principi generali	48
6.4.2	Consultazione ai fini giuridico-amministrativi	48
6.4.3	Consultazione per scopi storici	48
6.4.4	Consultazione da parte di personale interno all'amministrazione.....	49
7.	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.....	50
7.1	<i>Unicità del protocollo informatico.....</i>	50
7.2	<i>Registro giornaliero di protocollo.....</i>	50
7.3	<i>Registrazione di protocollo.....</i>	51
7.3.1	Documenti informatici.....	51
7.3.2	Documenti analogici (cartacei e supporti rimovibili).....	52
7.4	<i>Segnatura di protocollo dei documenti.....</i>	52
7.5	<i>Annullamento delle registrazioni di protocollo.....</i>	52
7.6	<i>Descrizione funzionale ed operativa del Sistema di Protocollo Informatico.....</i>	53
7.7	<i>Registrazioni di protocollo.....</i>	53
7.7.1	Attribuzione del protocollo	53
7.7.2	Registro informatico di protocollo	53
7.7.3	Tenuta delle copie del registro di protocollo	54
8.	RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI	55
8.1	<i>Generalità.....</i>	55
8.2	<i>Profili di accesso</i>	56
9.	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA	57
9.1	<i>Il registro di emergenza.....</i>	57
9.2	<i>Procedura di protocollazione in emergenza.....</i>	58
10.	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI	59
10.1	<i>Modalità di approvazione e aggiornamento del manuale.....</i>	59
10.2	<i>Regolamenti abrogati.....</i>	59
10.3	<i>Pubblicità del presente manuale</i>	59
10.4	<i>Operatività del presente manuale.....</i>	60
11.	ALLEGATI.....	61
11.1	<i>Normativa.....</i>	61
11.1.1	DPR 445/2000 - Articolo 53 (R) - Registrazione di protocollo	61

11.2	<i>Elenco AOO</i>	63
11.3	<i>Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi</i>	64
11.4	<i>Procedura per la protocollazione informatica sul Documentale MISE</i>	64
11.5	<i>Flusso documentale UCB</i>	64
11.6	<i>Procedure di gestione di flussi documentali specifiche delle Direzioni Generali</i>	64
11.7	Titolari d'archivio AOO	64
11.7.1	Titolario - Area Organizzativa: UFFICI DI DIRETTA COLLABORAZIONE DEL MINISTRO	64
11.7.2	Titolario - Area Organizzativa: AOO_INCENTIVI	64
11.7.3	Titolario - Area Organizzativa: AOO_AFFARI GENERALI	64
11.7.4	Titolario - Area Organizzativa: AOO_ATTIVITA' TERRITORIALI	65
11.7.5	Titolario - Area Organizzativa: AOO_COMUNICAZIONI	65
11.7.6	Titolario - Area Organizzativa: AOO_ENERGIA	65
11.7.7	Titolario - Area Organizzativa: AOO_INTERNAZIONALIZZAZIONE	65
11.7.8	Titolario - Area Organizzativa: AOO_POLITICHE INDUSTRIALI E TUTELA.....	65
11.8	<i>Piano di conservazione</i>	65
11.8.1	Massimario - Area Organizzativa: AOO_AFFARI GENERALI	65
11.9	<i>Procedura per la Protocollazione in Emergenza</i>	65

INDICE DELLE FIGURE

<i>Figura 1: flusso per PEC in entrata</i>	<i>37</i>
<i>Figura 2: flusso per PEC in uscita</i>	<i>38</i>
<i>Figura 3: Flusso della corrispondenza in entrata.....</i>	<i>41</i>
<i>Figura 4: Flusso della corrispondenza in uscita o interna alla AOO.....</i>	<i>42</i>

INDICE DELLE TABELLE

<i>Tabella 1: profili degli utenti con accesso al sistema di protocollo e gestione documentale.....</i>	<i>56</i>
<i>Tabella 2: Elenco AOO</i>	<i>63</i>
<i>Tabella 3: codici AOO per la protocollazione di emergenza</i>	<i>Errore. Il segnalibro non è definito.</i>

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), prevede per tutte le amministrazioni di cui all’art. 2 del decreto legislativo 30 marzo 2001, n. 165, l’adozione del Manuale di gestione.

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

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all’interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell’art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato 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, indipendentemente dal formato, 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 interni all’amministrazione stessa 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 e i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del titolario di classificazione e del massimario di selezione e di scarto;
- la modalità di accesso alle informazioni da parte di coloro che ne hanno titolo e interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

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

1.2 Ambito di applicazione del Manuale

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

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Ministero dello Sviluppo Economico a partire dal 1 Luglio 2016.

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 acronimi

Ai fini del presente Manuale si intende:

- per "**amministrazione**", il Ministero dello Sviluppo Economico (MiSE);
- per "**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per "**Regole tecniche**", il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428;

- per “**Codice**”, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell’amministrazione digitale.

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

- AOO - **A**rea **O**rganizzativa **O**mogenea;
- MdG - **M**anuale **d**i **G**estione del protocollo informatico e gestione documentale e degli archivi;
- PEC – **P**osta **E**lettronica **C**ertificata;
- RPA - **R**esponsabile del **P**rocedimento **A**mmministrativo - il dipendente che ha la responsabilità dell’esecuzione degli adempimenti amministrativi;
- RSP - **R**esponsabile del **S**ervizio per la tenuta del **P**rotocollo informatico, la gestione dei flussi documentali e degli archivi;
- PdP - **P**rodotto **d**i **P**rotocollo informatico – l’applicativo sviluppato o acquisito dall’amministrazione/AOO per implementare il servizio di protocollo informatico;
- UOP - **U**nità **O**rganizzative di registrazione di **P**rotocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- UOR - **U**ffici **O**rganizzativi di **R**iferimento - 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 - **U**fficio **U**tente - un ufficio dell’AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

1.4 Norme di riferimento

- Amministrazione digitale:
 - Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 – “Regole tecniche per il Protocollo Informatico di cui al DPR 428/98”;
 - Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – “Disposizioni legislative in materia di documentazione amministrativa”;
 - Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 – “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici”;

- Decreto Legislativo 7 marzo 2005, n. 82. – “Codice dell’Amministrazione digitale (CAD)”;
- Decreto del Presidente del Consiglio dei Ministri 22 luglio 2011 – “Comunicazioni con strumenti informatici tra imprese e Amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni”;
- 2014-Regole tecniche in materia di sistema di conservazione e Regole tecniche per il protocollo informatico, supplemento ordinario n. 20 della gazzetta ufficiale del 12/3/2014, n. 59;
- Posta elettronica certificata:
 - Decreto del Presidente della Repubblica 11 febbraio 2005, n.68. – “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”;
 - Circolare n. 1/2010/DDI – “Uso della Posta Elettronica Certificata nelle amministrazioni pubbliche”;
- Firma elettronica:
 - Decreto legislativo 23 gennaio 2002, n. 10 – “Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche”;
 - Decreto del Presidente della Repubblica 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”;
 - Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 – “Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici”;
- Sicurezza:
 - Decreto legislativo n.196 del 30 giugno 2003 – “Codice in materia di protezione dei dati personali”.

1.5 Aree Organizzative omogenee e modelli organizzativi

Per la gestione dei documenti, l’amministrazione ha adottato un modello organizzativo di tipo distribuito istituendo al suo interno le Aree Organizzative Omogenee (AOO). All’interno di ciascuna AOO è istituito un sistema di protocollazione unico ed un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'interno di ciascuna AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in ingresso e in uscita; in questo caso ogni UOR svolge anche i compiti di UOP.

L'elenco delle AOO è riportato nell'allegato 11.2, suscettibile di modifica in caso di inserimento di nuove AOO o di riorganizzazione delle medesime.

Nell'elenco sono riportati la denominazione e il codice identificativo per ogni AOO e la loro composizione.

1.6 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 anche RSP).

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 11.3, unitamente:

- alla denominazione del servizio;
- al nominativo del RSP.

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

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

1.7 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 e successivi aggiornamenti 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.

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 e al relativo consenso quando dovuto;
- alla nomina degli incaricati e responsabili del trattamento, per gruppo o individualmente;
- alle misure minime e idonee di sicurezza.

1.8 Caselle di posta elettronica

Le AOO sono dotate di caselle PEC divisionali per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Inoltre, in base alle esigenze, possono essere create caselle funzionali per procedimenti specifici.

In attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione dota tutti i propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, di una casella di posta elettronica.

1.9 Accredimento dell'amministrazione all'IPA

L'amministrazione/AOO si dota caselle di posta elettronica istituzionali attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; l'UOP medesima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

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

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

Il codice identificativo della amministrazione associato a ciascuna delle proprie AOO, è stato generato e attribuito autonomamente dall'amministrazione. L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito Internet da parte di tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione ovvero la creazione di una AOO.

1.10 Formazione

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

In particolare, considerato che il personale assegnato agli UOP deve conoscere sia l'organizzazione ed i compiti svolti da ciascun UOR/UU all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, sono stati previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

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

In considerazione della complessità e articolazione della materia trattata è stato definito un piano organico di formazione sull'argomento che si dovrà articolare con diverse modalità in base alle esigenze operative delle divisioni e agli utenti destinatari:

- corsi in aula;
- e-learning;

- seminari ai dirigenti;
- tutoring personalizzato ai direttori generali;
- tutoraggio on the job presso le singole direzioni generali per affrontare e risolvere le specifiche esigenze.

2. PIANO DI SICUREZZA

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

2.1 Obiettivi del piano di sicurezza

Il piano di sicurezza dei documenti informatici relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti stessi, contempla i seguenti aspetti:

- esecuzione dell'analisi dei rischi che incombono sui dati (personali e non) e/o sui documenti trattati;
- definizione delle politiche di sicurezza da adottare all'interno della AOO;
- pianificazione degli interventi da attuare in esito ai risultati ottenuti dalle attività precedenti;
- predisposizione, all'occorrenza, di piani specifici di formazione degli addetti;
- monitoraggio periodico del piano di sicurezza.

2.2 Generalità

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 idonee di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;

- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi o per altre motivazioni in cui l'amministrazione ritiene opportuno effettuare una modifica e/o aggiornamento del piano. 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 trimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- 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, degli applicativi e dei database;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

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

2.3 Formazione dei documenti - Aspetti di sicurezza

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

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

I documenti dell'A OO 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'A OO 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 A OO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

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

2.4 Gestione dei documenti informatici

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 l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.5 Trasmissione e interscambio dei documenti informatici

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 di cui si avvale l'amministrazione oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

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

2.6 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti definita in via preventiva.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo e/o l'applicativo.

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.

Per quanto riguarda gli 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.

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.

2.7 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11 "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali".

3. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

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

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.

3.1 Il documento informatico

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

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

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

3.2 Il documento analogico - cartaceo

Per documento analogico si intende un documento amministrativo "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, *microfiches*, *microfilm*), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale". Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o *text editor*) e poi stampata.

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

3.3 Formazione dei documenti - aspetti operativi

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.

Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale:

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

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

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR. Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso una o più delle seguenti informazioni:

- la denominazione e il logo dell'amministrazione;

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

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, 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 può rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

3.4 Requisiti degli strumenti informatici di scambio

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

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

- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

3.5 Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 3.4 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).

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.

3.5.1 Tipi di firma digitale

La vigente normativa prevede due tipologie di firma digitale che vengono denominati, per semplicità, "Firma p7m" e "Firma PDF"; entrambi i tipi di firma possono essere effettuati con tutti i dispositivi che contengono i certificati per la sua apposizione (firma remota, *smart card* o altro).

- Firma p7m: si possono firmare tutti i tipi di file (*word, excel, pdf, power point, ecc.*) e, a seguito dell'apposizione della firma digitale, l'estensione originaria del file viene trasformata in .p7m. I file .p7m si possono aprire solo attraverso un software di lettura e di verifica della firma; essa, comunque, non sarà visualizzabile in nessuna parte del documento. In questa modalità è possibile anche firmare diversi file contemporaneamente (firma massiva).
- Firma PDF: si possono firmare solo file in formato .pdf (PDF/A); in questo caso il certificato di firma digitale viene inserito all'interno del file e la firma è visibile immediatamente all'apertura del documento, senza necessità di software particolari dedicati alla lettura e verifica della firma. È anche possibile personalizzare il testo della firma che compare sul documento inserendo l'immagine della propria firma olografa o la motivazione di firma, ad es. "conforme all'originale conservato agli atti dell'ufficio" o "visto" o anche "per regolare esecuzione".

Nel file andranno, comunque, inserite le seguenti diciture:

In caso di documento nativo digitale	<i>“Documento sottoscritto con firma digitale ai sensi del D. Lgs. n. 82 del 7 Marzo 2005 e successive modifiche”</i>
In caso di documento cartaceo con firma olografa, scansionato e successivamente firmato digitalmente	<i>“Documento sottoscritto con firma digitale ai sensi del D. Lgs. n. 82 del 7 Marzo 2005 e successive modifiche. La copia è conforme all’originale cartaceo conservato agli atti dell’Ufficio”</i>

3.5.2 Dispositivi che contengono i certificati di firma

Il certificato digitale è l’elemento fondante della firma digitale, che garantisce l’identità di chi sta firmando e può essere installato/contenuto in diversi dispositivi (firma remota, *smart card* o altro) che consentono sia la tipologia “Firma PDF” sia quella “Firma p7m”.

- In caso di uso della *smart card* il certificato è memorizzato nel dispositivo stesso. Nell’immediato futuro verrà introdotta sul SICOGE la firma digitale dei mandati. Tale funzione è disponibile solo tramite *smart card*.
- In caso di uso della firma remota (firma.mise.gov.it) il certificato è installato nel server. I sistemi mobili, quali *tablet* o *smartphone*, non possono utilizzare le *smart card*, quindi, possono usare solo firme remote.

3.5.3 Generazione dei documenti pdf e pdf ricercabili

I documenti digitali in formato PDF possono essere generati sia tramite la scansione di un documento sia direttamente da Word o prodotti simili con la procedura “Salva con nome -> tipo file:PDF” (PDF/A). Questa funzionalità potrebbe non essere disponibile in versioni non recenti degli applicativi.

In questo secondo caso vengono creati PDF cosiddetti “ricercabili” nei quali è possibile ricercare e copiare il testo. Nel caso della scansione, diversamente, il PDF è costituito da una immagine e, esclusivamente attraverso programmi dedicati alla conversione dell’immagine in testo (*OCR - optical character recognition*) è possibile effettuare la ricerca testuale all’interno del documento.

Si rammenta, inoltre, che la scansione di un documento produce un file .pdf di maggiori dimensioni rispetto ad un file word salvato in .pdf.

3.5.4 Marcatura temporale

In ordine alla validità temporale del documento firmato digitalmente, qualora esso sia stato firmato da un computer connesso alla rete del Ministero, la data e l'ora sono automaticamente sincronizzate con il segnale dell'orologio atomico dell'Istituto Galileo Ferraris. In ogni caso, la protocollazione del documento sul sistema di Protocollo Informatico del Ministero sostituisce la marcatura temporale.

3.5.5 Documenti informatici e protocollazione

L'archiviazione dei documenti informatici è valida solo se effettuata su sistemi di gestione documentale come ad es. il sistema di gestione documentale e protocollo del MISE; quindi la sua conservazione cartacea (ovvero tramite stampa del documento) non ha valore giuridico.

Si ricorda che le AOO - Aree Organizzative Omogenee - devono utilizzare per le comunicazioni interne al Ministero i seguenti strumenti messi a disposizione ai fini della dematerializzazione ovvero:

- tra le AOO, l'invio tramite PEC di documenti protocollati;
- all'interno delle AOO, tramite la funzione di assegnazione del documento attraverso il sistema di gestione documentale/protocollo.

Sull'argomento si rinvia alla circolare UAGR n. 1682 del 13/11/2012 - "Procedura per la protocollazione dei messaggi di posta elettronica certificata (PEC)".

3.5.6 Copie e trasmissione di documenti informatici

Se si deve trasmettere in forma ufficiale cartacea un documento firmato digitalmente è necessario stamparlo ed attestare che la copia cartacea è conforme all'originale digitale. Se, invece, la necessità è quella di trasmettere in forma digitale un documento cartaceo, si deve scansionare quello con firma olografa e firmare il PDF così generato apportando la dicitura precedentemente indicata ("Documento sottoscritto con firma digitale ai sensi del D. Lgs. n. 82 del 7 Marzo 2005 e successive modifiche. La copia è conforme all'originale cartaceo conservato agli atti dell'Ufficio").

Ogni copia informatica di un documento firmato digitalmente costituisce originale. La stampa di un documento firmato digitalmente (sia con Firma .p7m sia con Firma .PDF) non può sostituire l'originale e non ne rappresenta copia valida; l'originale resta comunque il documento digitale e come tale deve essere gestito e conservato nel sistema di gestione informatica dei documenti per garantirne l'autenticità.

Per la trasmissione e la diffusione a terzi di un documento firmato digitalmente è possibile procedere in diversi modi: utilizzando la PEC e il protocollo informatico ma anche la normale email, una penna USB o il caricamento del documento su un sito intranet o Internet. In nessun caso il documento perde di validità.

3.5.7 Gli strumenti forniti dal MISE

Atteso l'elevato numero di strumenti disponibili per l'apposizione, la gestione della firma digitale e quella documentale, si descrivono di seguito quelli ufficialmente forniti dal MISE e in uso internamente, segnalando, altresì, la probabile futura evoluzione della tecnologia in materia che potrà portare alla diffusione di successivi aggiornamenti della presente nota.

Firma digitale

È fornita a tutti i dirigenti e, su richiesta, ai funzionari dotati di delega di firma; la perdita del supporto di firma (*smart card*) deve essere denunciata all'Autorità Giudiziaria e comunicata all'amministrazione stessa.

Il MISE dispone sia di sistemi di firma remota sia di firma con *smart card*, ma sarà dato massimo impulso all'utilizzo della firma remota in quanto maggiormente integrabile negli applicativi quali il Documentale MISE.

Su tutti i *computer*, a prescindere che si sia in possesso di firma digitale o meno, dovranno essere installati i *software* DikePDF e Acrobat Reader correttamente configurati per poter leggere i documenti firmati digitalmente e verificare sia Firme p7m sia Firme PDF.

È possibile procedere alla firma contemporanea (firma massiva) di più atti con *smart card* esclusivamente con la Firma p7m utilizzando il *software* File Protector.

Per le installazioni e le configurazioni necessarie sarà possibile utilizzare l'applicativo "Assistenza informatica" presente in intranet nella sezione "Servizi Web"

PEC

Il MISE predispone le caselle di PEC per tutte le strutture organizzative del Ministero, ovvero Direzioni generali, divisioni, unità organizzative. La PEC equivale ad una Raccomandata con ricevuta di ritorno.

Tutte le caselle PEC sono configurate nel sistema di protocollo per la gestione informatica dei documenti (art. 40-bis del CAD) Documentale MISE e la ricezione e gli invii dovranno essere effettuati tramite il protocollo informatico stesso.

Per le configurazioni necessarie sarà possibile utilizzare l'applicativo "Assistenza informatica" presente in intranet nella sezione "Servizi Web"

Per attivare, su motivata richiesta, ulteriori caselle PEC si fa riferimento alla recente circolare in materia (DGROB prot. n. 3078 del 13/02/2015). Per ogni nuova richiesta deve essere utilizzato l'applicativo "Assistenza informatica" presente in intranet nella sezione "Servizi Web"

Sistema di Gestione Documentale e Protocollo

Il sistema, comune a tutto il MISE, è attivo presso ogni struttura. Tutto il personale è già abilitato come utente documentale o secondo i profili operativi richiesti ai Referenti tecnici di AOO delle Direzioni generali. Il sistema consente la protocollazione delle PEC in ingresso e uscita, con relative ricevute di consegna e accettazione, e la loro successiva gestione.

3.6 Verifica delle firme con il PdP

Nel PdP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare. Tale verifica è effettuata in modo conforme alla Deliberazione CNIPA 21 maggio 2009, n. 45.

3.7 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. 2.5).

Allo scopo di effettuare la trasmissione di un documento ad un'altra Amministrazione oppure ad altra/altra AOO utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni nel sistema Documentale MISE:

- inserire il documento, redatto con un sistema di videoscrittura, in un fascicolo (eventuale);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato);

- inserire i dati del destinatario (almeno denominazione, casella di posta elettronica); per gli scambi tra AOO del MISE è possibile reperire tali dati dall'apposito tasto "Uffici AOO ente"
- protocollare in uscita il documento firmato digitalmente; contestualmente il sistema documentale MISE provvederà ad 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) per i documenti firmati elettronicamente consente di:

- inviare documenti originali digitali;
- 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 gestione nel Documentale MISE delle ricevute di consegna e accettazione o di eventuali eccezioni generati dal sistema di posta certificata. Ciascun messaggio protocollato e inviato per PEC genera una ricevuta di accettazione e tante ricevute di consegna quanti sono i destinatari. .

I messaggi di ritorno, oltre alle ricevute di accettazione e consegna, possono essere, ad es.:

- conferma di ricezione;
- notifica di eccezione;
- aggiornamento di conferma;
- ricevuta di protocollo;
- 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 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.

4. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

Per ulteriori approfondimenti è possibile rivolgersi a: dgrob.documentale@mise.gov.it. Allegato 11.4.

4.1 Generalità

In considerazione delle recenti disposizioni normative rivolte al risparmio della spesa nonché dei dettami del Codice dell'amministrazione digitale (CAD, D. Lgs. 7/3/2005, n.82 e successivi aggiornamenti) che sanciscono la riduzione del cartaceo e l'utilizzo delle trasmissioni con la PA tramite PEC, si definiscono le seguenti procedure operative.

Il sistema di protocollo e gestione documentale MISE prevede la possibilità di protocollare, in Ingresso e in Uscita, i messaggi di posta elettronica certificata (PEC) collegandosi direttamente con le caselle di posta degli uffici. I documenti possono essere direttamente protocollati dal Documentale MISE mantenendo inalterata la loro natura di documenti nativi digitali ed inseriti nel sistema di gestione dei documenti per la loro trattazione (Registro di protocollo, assegnazioni, fascicolazione).

Si forniscono a tal proposito le seguenti indicazioni:

- in considerazione della fornitura delle caselle di PEC a tutte le Divisioni del Ministero si è ritenuto di adottare, per la protocollazione di mail certificate, il modello organizzativo del protocollo federato ovvero la protocollazione dei documenti, in ingresso ed in uscita, sarà decentrata presso le strutture responsabili della gestione delle caselle di PEC (Dipartimenti, Direzioni generali, Divisioni, Unità organizzative, procedimenti amministrativi). Il sistema è predisposto anche per la protocollazione centralizzata dei documenti elettronici ma questo comporta delle difficoltà organizzativo-gestionali che potranno essere valutate solo caso per caso, dove se ne riscontri l'esigenza;
- in considerazione dell'utilizzo in tutto il Ministero dello stesso sistema di protocollo e gestione documentale, si invitano le AOO-Aree Organizzative Omogenee ad utilizzare per le comunicazioni interne al MISE i seguenti strumenti a disposizione per la riduzione dell'inoltro cartaceo, a meno di particolari esigenze amministrative:
 - tra le AOO, l'invio tramite PEC di documenti protocollati;

- all'interno delle AOO, tramite la funzione di assegnazione del sistema di gestione documentale/protocollo (modalità interna, per lo scambio tra Direzioni generali e/o divisioni di una stessa Direzione).

4.2 Procedura per la protocollazione dei messaggi di Posta Elettronica Certificata (PEC)

La protocollazione dei messaggi di PEC si effettua attraverso l'accesso al Documentale MISE, per il quale si forniscono alcune indicazioni:

- Le caselle PEC sono configurate per scaricare automaticamente i messaggi nel Sistema di gestione documentale e protocollo, unico canale per la loro visualizzazione. Su richiesta è configurabile anche lo scarico dei messaggi nel protocollo dopo che sono stati visionati. La corretta trattazione dei documenti informatici si basa sulla gestione completamente digitale, senza ricorrere alla stampa, dei documenti giunti tramite mail;
- per consentire la protocollazione delle PEC è necessario attribuire il Profilo di Protocollatore I/U + PEC oppure Protocollatore Riservato;
- per visualizzare file firmati digitalmente con estensione .p7m è necessario che sul PC sia installato un programma specifico (es. Dike);
- le caselle PEC di divisione (ai sensi dell'art. 47 co 3 D.Lgs. 82/2005 - CAD) sono inserite di default nel Documentale ed utilizzate ai fini della protocollazione, è possibile richiedere l'inserimento anche delle caselle dedicate a procedimenti specifici;
- in considerazione della fornitura delle caselle di PEC a tutte le Divisioni del Ministero si è ritenuto di adottare il modello organizzativo del protocollo federato: la protocollazione dei documenti, in ingresso ed in uscita, sarà decentrata presso le strutture responsabili della gestione delle caselle di PEC (Dipartimenti, Direzioni generali, Divisioni, Unità organizzative, procedimenti amministrativi);
- le caselle PEC del MISE sono di norma configurate per ricevere solo da altre caselle PEC;
- per i messaggi soggetti a protocollazione ricevuti su casella non PEC, è opportuno inviare una mail di risposta al mittente per la ritrasmissione del messaggio alla casella PEC;
- i messaggi giunti su una casella PEC e re-inoltrati ad un'altra casella PEC non saranno gestiti correttamente dal sistema, quindi la protocollazione e successiva assegnazione dovrà essere effettuata dal primo destinatario PEC interno al ministero;
- l'utilizzo di tali caselle è legato alla creazione delle cartelle di ricezione, collegate con le liste di competenza (ACL). Ad es. creando liste di competenza coincidenti con le divisioni, ogni casella di divisione scarica le mail sulla cartella di ricezione accessibile alla lista di

competenza formata dal personale della divisione stessa e l'accesso tramite protocollo è legato all'abilitazione come Protocollore I/U+PEC.

4.3 Flussi procedurali per la protocollazione delle PEC

4.3.1 PEC in entrata

Nell'ottica della ricerca della soluzione organizzativa più congeniale all'operatività delle strutture, le singole Direzioni Generali possono predisporre, per le PEC in ingresso, la protocollazione accentrata presso un Ufficio centrale di protocollo piuttosto che la protocollazione decentrata presso le singole Divisioni responsabili delle caselle.

L'Ufficio di protocollo/Protocollore I/U+PEC provvede:

- alla protocollazione delle mail in ingresso indirizzate alla/e caselle PEC di competenza ;
- all'assegnazione sul sistema di gestione documentale MISE alla/e Divisioni destinatarie; in caso di dubbi sarà assegnata alla Segreteria per il seguito di competenza. Qualora una PEC fosse indirizzata a più divisioni l'ufficio di protocollo provvederà ad effettuare la protocollazione per una divisione e l'assegnazione per le altre divisioni destinatarie per evitare duplicazioni di protocollo.
- il sistema invia al dirigente una mail di notifica di ogni assegnazione effettuata.

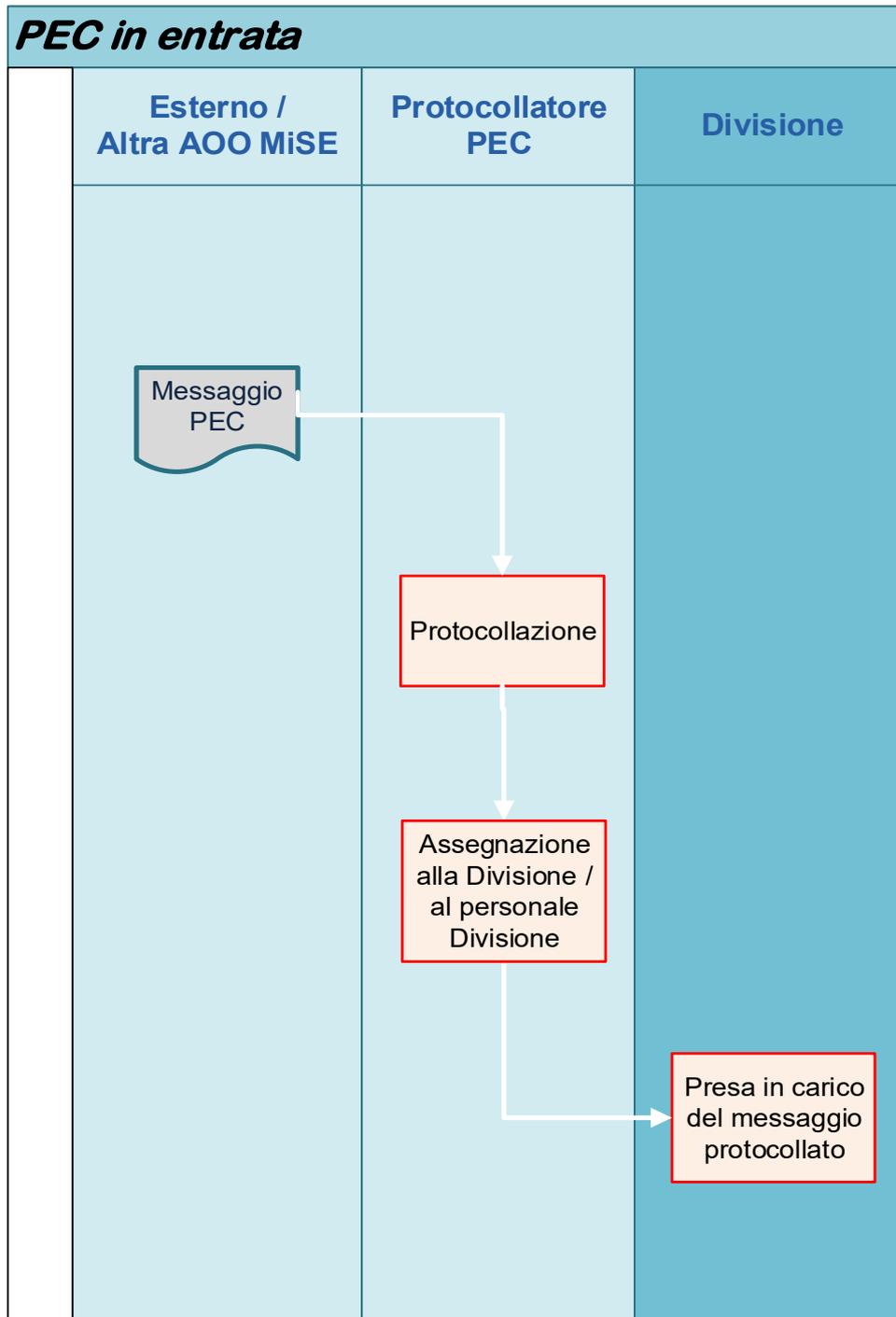


Figura 1: flusso per PEC in entrata

4.3.2 PEC in uscita

In considerazione della facilitazione apportata al flusso lavorativo dalla funzione di protocollazione e contestuale invio, per l'uscita si è scelto il modello organizzativo del protocollo federato ovvero la protocollazione decentrata dei documenti presso le singole divisioni, eventualmente l'ufficio di

protocollo centralizzato potrà fornire il supporto operativo. Il sistema effettua contestualmente l'operazione di protocollazione dei documenti informatici ed il loro invio tramite PEC; il protocollo sarà così generato e inviato all'interno del sistema di gestione documentale.

Si ricorda che, in base ai dettami normativi, i documenti informatici inviati per PEC andranno firmati digitalmente; se alcuni funzionari sono delegati alla firma dal Dirigente, su richiesta si fornirà loro la firma digitale.

Per la protocollazione non sono necessari etichettatrice e scanner in quanto i documenti digitali non dovranno essere stampati né scansionati.

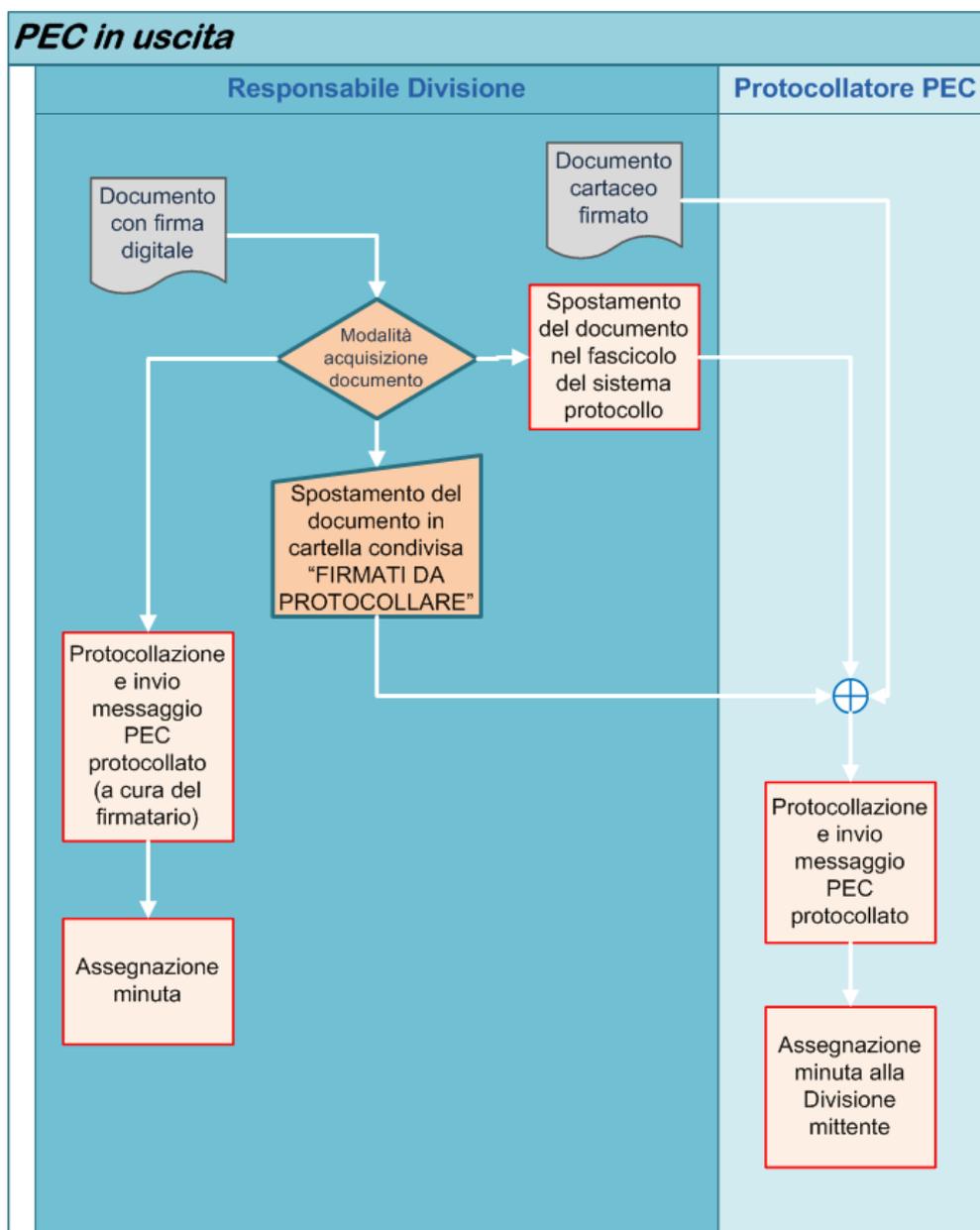


Figura 2: flusso per PEC in uscita

Si distinguono le due tipologie di documento:

- documento originale informatico (firmato digitalmente):
- documento originale cartaceo:
 - scansione firmata con firma digitale, valore giuridico del documento originale (copia conforme);
 - scansione senza firma digitale, valore probatorio liberamente valutabile in giudizio.

Per acquisire sul sistema di protocollo i file firmati digitalmente si può procedere nei seguenti modi alternativi, in base alle procedure operative adottate dalle divisioni:

- caricamento da PC: il firmatario (che possiede anche il ruolo di protocollatore I/U + PEC) carica direttamente il file dal suo PC durante la procedura di protocollazione sul sistema di protocollo;
- caricamento da cartella di rete condivisa: il firmatario deposita il file in una cartella condivisa (“Firmati da protocollare”) accessibile ai protocollatori I/U + PEC, che procederanno alla protocollazione sul sistema di protocollo. La creazione della cartella condivisa dovrà essere richiesta tramite l’applicativo “Assistenza informatica” presente in intranet nella sezione “Servizi Web”
- caricamento dal sistema di protocollo/gestione documentale: il firmatario inserisce il file in un fascicolo predisposto sul sistema, una volta protocollato il file verrà sostituito nel fascicolo con quello timbrato.

Il protocollatore I/U + PEC procederà a questo punto alla protocollazione dei documenti sul sistema di protocollo.

4.4 Flussi procedurali per la protocollazione dei documenti cartacei

Esempio di organizzazione con la presenza dell’Ufficio centrale di protocollo di Direzione.

4.4.1 *Protocollazione in entrata*

La Segreteria del Direttore generale riceve la documentazione in arrivo e provvede:

- all’apposizione del timbro di arrivo;
- alla ripartizione tra le Divisioni in base alle competenze;
- all’invio all’Ufficio di protocollo.

L'ufficio centrale di Protocollo, previa verifica della presenza del timbro di arrivo apposto dalla Segreteria e in base alle eventuali indicazioni presenti sul cartaceo, effettua sul sistema le seguenti operazioni:

- protocollazione della documentazione con la scansione dell'intero documento;
- classificazione, quando possibile;
- assegnazione informatica alle Divisioni.

I documenti vengono depositati nelle cassette di competenza delle varie Divisioni.

Le Divisioni provvedono:

- al ritiro e alla gestione della documentazione cartacea protocollata; qualora sorgano dubbi sulla competenza alla trattazione, la relativa corrispondenza sarà rimessa alla decisione del Direttore generale, segnalando le relative motivazioni;
- alla presa in carico della documentazione sul sistema di gestione documentale MISE; riassegnazione interna ai singoli utenti, classificazione e fascicolazione come in seguito specificato (vedi sezione Gestione documentale).

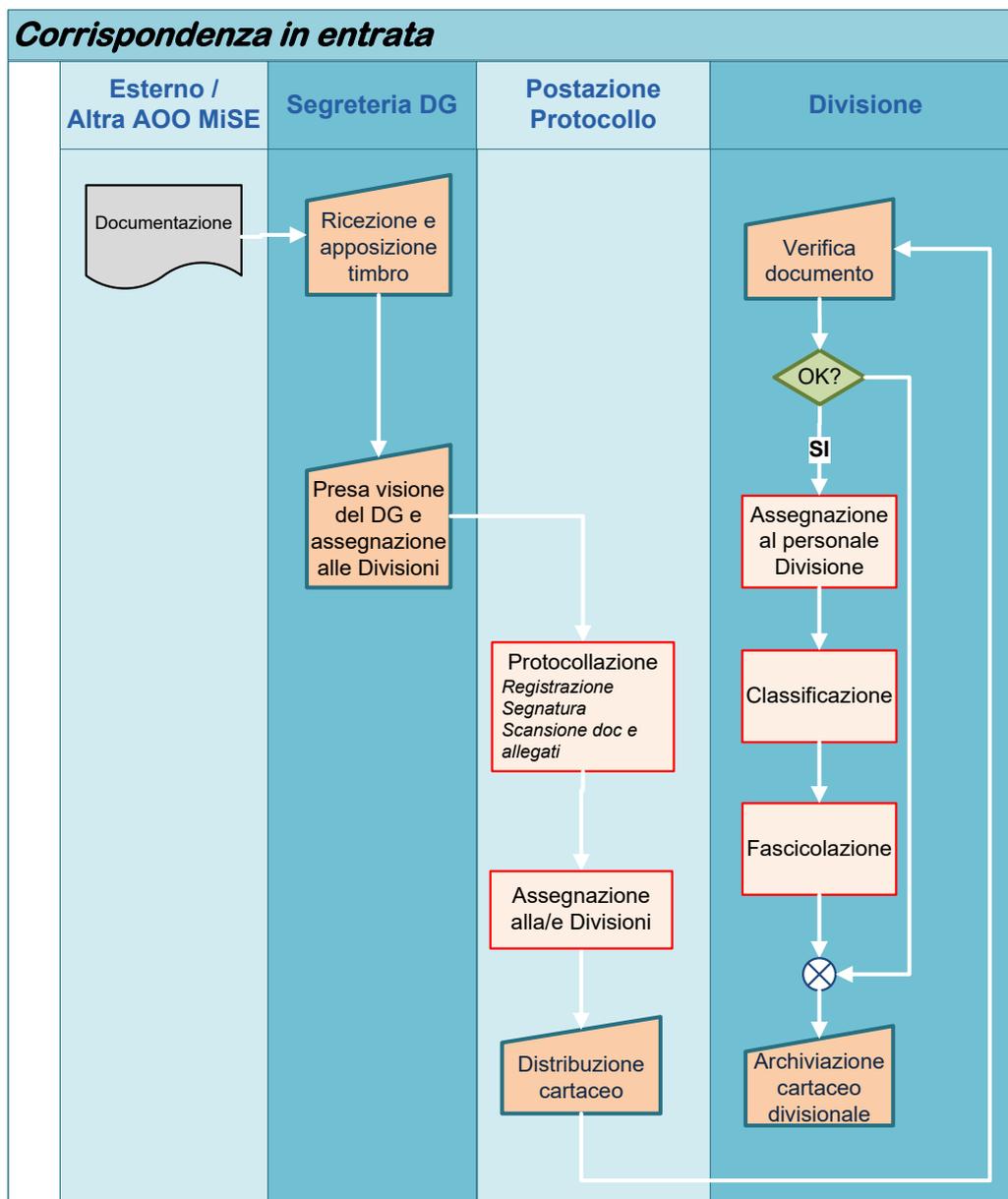


Figura 3: Flusso della corrispondenza in entrata

4.4.2 *Protocollazione in uscita o interna*

Ogni Divisione si occupa della preparazione della pratica per la protocollazione e della consegna al servizio di protocollo (Rif. Disposizioni Prot.n. 1644, 6/11/2012-RI UAGR).

L'ufficio centrale di Protocollo provvede:

- alla protocollazione con la scansione dell'intero documento comprensivo degli allegati;
- alla classificazione, in base al codice di Titolare inserito dall'autore in calce al documento, elemento questo obbligatorio ai fini della protocollazione;

- all'imbustamento e spedizione della documentazione;
- all'assegnazione del formato elettronico attraverso il sistema di protocollo: - alle divisioni destinatarie interne; - a quella mittente, come minuta; - all'autore del documento, ove indicato (a piè di pagina).

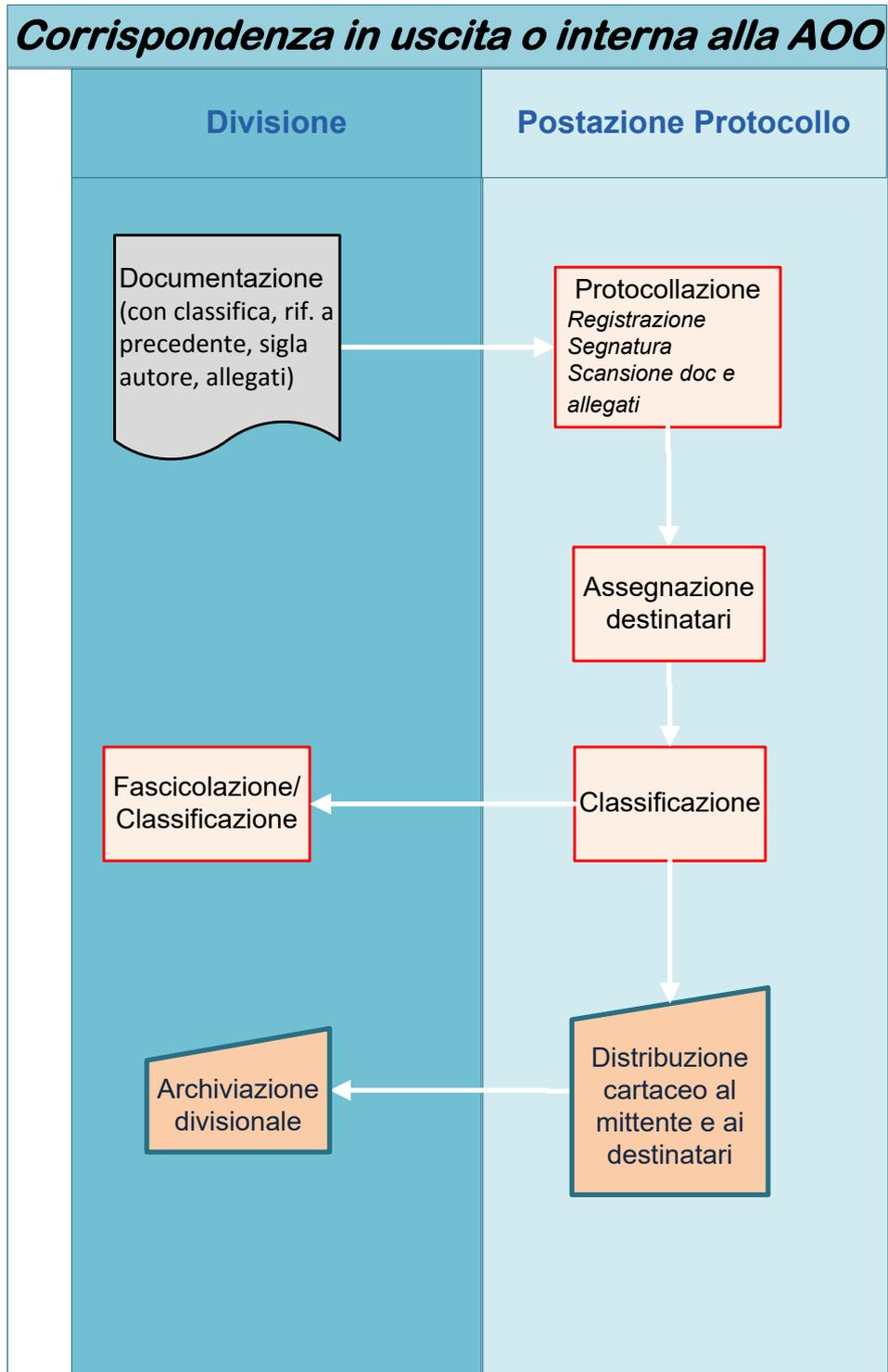


Figura 4: Flusso della corrispondenza in uscita o interna alla AOO

4.5 Procedura Flusso UCB

In ottemperanza alle previsioni normative sulla dematerializzazione degli atti amministrativi, il Ministero ha provveduto a sviluppare all'interno del Documentale MISE le nuove funzioni per l'invio digitale all'UCB dei provvedimenti, sono infatti state ampliate le funzionalità del protocollo informatico per includere le informazioni necessarie al dialogo applicativo con i sistemi della Ragioneria, sia in caso di impegno che di pagamento.

Con riferimento alle procedure di acquisto e di pagamento, la conservazione dei documenti istruttori e la loro validità temporale, sarà garantita tramite la protocollazione degli stessi e dei relativi allegati. Tali atti, che dovranno essere nelle forme digitali previste dalla circolare cui si fa riferimento, dovranno obbligatoriamente essere inseriti nel fascicolo digitale unitamente ai provvedimenti di impegno e pagamento al fine di predisporre la conservazione sostitutiva a norma.

Nell' [allegato 11.5](#) la circolare Prot.n. RU 10065, del 6/5/2016, sull'Avvio del flusso dematerializzato di invio dei documenti all'UCB MISE" (e successive modifiche), contenente la procedura da seguire per la protocollazione e l'invio all'UCB.

4.6 Procedure di gestione di flussi documentali specifiche delle Direzioni Generali

Le procedure gestionali verticali finalizzate a procedimenti di competenza delle Direzioni Generali o modifiche ai flussi generali previsti dal presente Manuale saranno presentate in Allegato ad opera dei responsabili delle AOO per le DG di appartenenza. [Allegato 11.6.](#)

5. ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

5.1 Documenti esclusi

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

5.2 Documenti soggetti a registrazione particolare

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa (documentazione sensibile);
- le tipologie di documenti individuati dalla normativa vigente (in particolare dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352 e dalla serie di norme collegate alla legge 31 dicembre 1996, n. 675 e successive modificazioni).

E' possibile:

- indicare l'apposita opzione di protocollazione riservata da spuntare a cura del protocollatore riservato nell'ambito del Registro ufficiale. Tale opzione garantisce che l'accesso al documento sia possibile solo al personale strettamente preposto all'espletamento della pratica.
- prevedere l'apertura di un Registro riservato, le tipologie di documenti da registrare nel protocollo riservato sono individuate dal responsabile del protocollo informatico/Organizzazione in collaborazione con i responsabili delle UOR. Il particolare Registro riservato è utilizzato, in linea di massima, mediante procedure particolari con accesso riservato, con livelli di accesso stabiliti caso per caso.

Entrambi i tipi di registrazione consentono comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertorizzazione.

6. IL SISTEMA DI CLASSIFICAZIONE

6.1 Protezione e conservazione degli archivi pubblici

6.1.1 Generalità

Il presente capitolo riporta il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, 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.

6.1.2 Misure di protezione e conservazione degli archivi pubblici

L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità. Il trasferimento ad altre persone giuridiche di complessi organi 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.

6.2 Classificazione dei documenti, Titolario e Piano di conservazione

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 titolare 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 titolare. Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse, etc.), il numero del fascicolo ed eventualmente del sotto-fascicolo.

Qualora l'ente lo ritenga opportuno, le operazioni di classificazione possono essere svolte in momenti diversi: demandata al Protocollore o all'Utente documentale incaricato della trattazione della pratica.

6.2.1 Titolario

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

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

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

Dopo ogni modifica del titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

Per il MISE si è scelto di condividere tra tutte le AOO le prime 9 voci di carattere generale, afferenti alle competenze trasversali (staff); ogni AOO accoderà le proprie voci di competenza specifica. Fanno parte del Titolario anche le indicazioni di fascicolazione, relative per ogni voce alle specifiche di creazione dei fascicoli/sottofascicoli, al contenuto da inserire, alle indicazioni di conservazione. In Allegato un esempio.

In [Allegato 11.7 sono](#) inseriti i titolari delle AOO, opportunamente aggiornati.

6.2.2 Piano di conservazione

Il Massimario di selezione e scarto definisce le tempistiche legate alla gestione dei documenti presenti in archivio. In [Allegato 11.8](#)

Per quelle AOO per cui il massimario è stato già definito la DGROB formalizza l'impiego di detto massimario all'interno dell'amministrazione medesima con l'aggiornamento sul presente Manuale.

Per le AOO per cui non è stato ancora definito il massimario di scarto, questo viene proposto dal RSP, 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.

Ogni AOO nel definire le voci di competenza specifica individua anche le indicazioni relative alla conservazione dei documenti, per lo scarto o il riversamento agli archivi di stato competenti per territorio.

Dovei tempi non fossero ancora indicati si considera un tempo di conservazione di 10 anni.

6.3 Scarto, selezione e riordino dei documenti

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

Le operazioni di selezione e scarto sono effettuate dalle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato, come nominate dalle singole AOO/Direzioni Generali. I documenti e gli atti sottoposti a procedura di scarto sono devoluti gratuitamente secondo quanto stabilito dal decreto del Presidente della Repubblica del 8 gennaio 2001, n. 47 art. 84.

[Rif.: D.P.R. dell'8 gennaio 2001, n. 37 Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato (n. 42, allegato 1, della L. n. 50/1999)]

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

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita dall'amministrazione/AOO e consiste nella schedatura dei materiali e nell'organizzazione delle schede. L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (scatole, pallets, etc.) che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti.

6.3.3 *Versamento dei documenti nell'archivio storico*

Gli organi giudiziari e amministrativi dello Stato versano all'Archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre quarant'anni, unitamente agli strumenti che ne garantiscono la consultazione. Nessun versamento può essere ricevuto se non sono state effettuate le operazioni di scarto. Le spese per il versamento sono a carico delle amministrazioni versanti.

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

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

6.4.1 *Principi generali*

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

6.4.2 *Consultazione ai fini giuridico-amministrativi*

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

6.4.3 *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.

6.4.4 Consultazione da parte di personale interno all'amministrazione

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

7. 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.

7.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal 1° 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.

La documentazione non registrata 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.

7.2 Registro giornaliero di protocollo

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendo la non modificabilità del contenuto.

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

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili i quali sono conservati in luogo sicuro a cura del responsabile della conservazione delle copie, appositamente nominato dall'amministrazione/AOO diverso dal RSP ai sensi dell'art. 7 comma 5 del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000.

7.3 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). La procedura completa è disponibile nella sezione degli allegati, al paragrafo 11.4.

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.

7.3.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'amministrazione. La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.

Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

7.3.2 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.

7.4 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.

La segnatura di protocollo, sia per quanto riguarda i documenti informatici che quelli cartacei, è fatta in maniera conforme a quanto stabilito dalla circolare AGID n. 60 del 23 gennaio 2013.

7.5 Annullamento delle registrazioni 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.

7.6 Descrizione funzionale ed operativa del Sistema di Protocollo Informatico

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

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

Le funzionalità del sistema informatico sono dettagliate nei manuali del sistema stesso. I singoli processi di lavoro sono documentati individualmente. I manuali sono disponibili nel sistema Documentale MISE alla voce Aiuto.

7.7 Registrazioni di protocollo

7.7.1 *Attribuzione del protocollo*

Al fine di assicurare la non modificabilità 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.

7.7.2 *Registro informatico di protocollo*

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO il sistema Documentale Mise attiva un processo automatico che genera il registro giornaliero del Registro Ufficiale e lo invia dalle mail istituzionali delle AOO alla casella PEC del nominativo indicato come responsabile dell'AOO, per la quale è stato attivato il servizio di conservazione sostitutiva.

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.

7.7.3 Tenuta delle copie del registro di protocollo

Le modalità di gestione di tali supporti sono definite e regolamentate direttamente dal RSP dell'AOO. I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.

8. 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.

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

Tutto il personale MISE è inserito nel ruolo di Utente documentale per poter gestire la documentazione amministrativa. I diversi livelli di autorizzazione possono essere attribuiti dal Referente tecnico di AOO competente o richiesti tramite l'applicativo "Assistenza informatica" presente in intranet nella sezione "Servizi Web"

8.2 Profili di accesso

Di seguito vengono riportati i profili degli utenti con accesso al sistema di protocollo e gestione documentale MiSE.

Tabella 1: profili degli utenti con accesso al sistema di protocollo e gestione documentale

Profilo	Ruoli
Amministratore	Amministratore di Sistema MISE
Referente tecnico AOO	Amministratore di AOO
Protocollatore Responsabile	Protocollazione (I/U/PEC), fascicolazione, annullamento dei protocolli
Protocollatore Riservato	Protocollazione riservata (I/U/PEC), fascicolazione, annullamento dei protocolli
Protocollatore I/U + PEC	Protocollazione (I/U/PEC), fascicolazione.
Protocollatore I/U	Protocollazione (I/U), fascicolazione.
Protocollatore Uscita	Protocollazione (U+U PEC), fascicolazione.
Utente firmatario	Utente documentale con diritto di firma digitale
Utente Documentale AOO	Gestione documentale (assegnazione-presenza in carico, ricerca/lettura dei Registri di protocollo della AOO, fascicolazione)
Utente documentale	Gestione documentale (assegnazione-presenza in carico, ricerca/lettura dei Registri di protocollo dell'ufficio, fascicolazione)
Consultatore storico	Ricerca/lettura dei Registri di protocollo delle AOO chiuse

9. 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.

9.1 Il registro di emergenza

Ogni qualvolta, per motivi accidentali o programmati, non fosse possibile utilizzare il sistema informatico per le attività di protocollazione per un periodo di tempo significativo, il RDS emette una dichiarazione, che sarà mantenuta agli atti, nella quale indica, con esattezza, la data e l'ora di inizio del non funzionamento e il relativo motivo.

Durante il periodo di non funzionamento del sistema informatico non sarà possibile protocollare documenti informatici in ingresso, poiché tale attività è strettamente correlata alle funzionalità del sistema stesso.

Se, invece, tra i documenti analogici pervenuti, venisse riscontrato un atto che per la sua rilevanza fosse necessario protocollare immediatamente, si procederà al suo inserimento nel registro di emergenza, provvedendo alla trasmissione del medesimo all'UO di competenza.

Per quanto riguarda l'uscita di documentazione digitale, essendo possibile solo attraverso l'apposizione della firma digitale e tramite la posta elettronica, non sarà disponibile.

Se vi fosse un atto che per la sua rilevanza dovesse comunque essere trasmesso, verrà prodotto con metodologie alternative dall'UO di competenza e portato all'attenzione del RDS per la relativa protocollazione di emergenza e successiva trasmissione per canali analogici. Appare evidente che non è conveniente procedere con tali modalità ed è buona norma ridurre al minimo indispensabile l'accesso a tali funzioni.

Vale anche la pena di sottolineare che l'eventuale mancato funzionamento del sistema inibisce anche l'accesso all'archivio informatico e alle funzioni di ricerca in generale, determinando il sostanziale blocco operativo dell'AOO.

Quando il sistema informatico riprende il suo normale funzionamento, il RDS produce una ulteriore dichiarazione, con l'esatta indicazione della data e dell'ora della ripresa del servizio.

Tutte le dichiarazioni del RDS di attivazione e chiusura del registro di emergenza sono conservate a cura del RDS.

Dopo la riattivazione i documenti in ingresso protocollati in emergenza, verranno immessi all'interno del sistema con le usuali metodologie. Parimenti si riprodurranno, a cura delle UO di competenza, i documenti protocollati in emergenza in uscita, con l'accortezza di farli confluire all'interno della lista dei documenti da materializzare: tale azione consentirà di disporre del nuovo numero di protocollo senza la necessità di ritrasmettere il documento stesso.

Il numero di protocollo assegnato ai documenti con il registro d'emergenza verrà trascritto a cura degli operatori che si occuperanno della nuova produzione nel sistema informatico nei campi previsti (Note/decretazioni).

9.2 Procedura di protocollazione in emergenza

A norma dell'Art.63 - DPR 445, le protocollazioni in emergenza possono essere effettuate sia con la modalità informatica sia con quella manuale, la modalità sarà decisa dal Responsabile del Servizio di gestione documentale e archivi. Il protocollo sarà per le pratiche urgenti così come individuate dalle Direzioni Generali. Nell' Allegato 11.9 la relativa procedura.

10. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

10.1 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, e gli allegati che ne costituiscono parte integrante, potrà essere aggiornato a seguito di:

- normativa specifica sopravvenuta;
- modifiche organizzative del Ministero;
- 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.

10.2 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.

10.3 Pubblicità del presente manuale

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

- pubblicata sulla rete intranet per tutto il personale delle AOO, Intranet—Aree—Gestione informatica dei documenti—Manuale di gestione;
- pubblicata sul sito internet dell'amministrazione.

10.4 Operatività del presente manuale

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

11. ALLEGATI

11.1 Normativa

11.1.1 DPR 445/2000 - Articolo 53 (R) - Registrazione di protocollo

- La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni e' effettuata mediante la memorizzazione delle seguenti informazioni:
 - numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
 - data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
 - mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
 - oggetto del documento, registrato in forma non modificabile;
 - data e protocollo del documento ricevuto, se disponibili;
 - l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
- il sistema deve consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno;
- l'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.
- con decreto del Presidente del Consiglio dei Ministri, su proposta dell'Autorità per l'informatica nella pubblica amministrazione di concerto con il Ministro per la funzione pubblica, sono specificate le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione di protocollo;
- sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle

circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

11.2 Elenco AOO

Denominazione dell'Amministrazione	Ministero dello sviluppo economico (MISE)
Codice identificativo	MISE
Indirizzo sede principale	Via Molise 2 – 00187 - Roma
Elenco delle AOO	
AOO Uffici diretta collaborazione Ministro (AOO_UDCM)	Uffici diretta collaborazione Ministro (UDCM)
AOO Affari generali (AOO_AG)	Segretariato generale (SG)
	DG Risorse, organizzazione e bilancio (DG ROB)
AOO_Energia (AOO_ENE)	DG Sicurezza anche ambientale delle attività minerarie ed energetiche - Ufficio nazionale minerario per gli idrocarburi e le georisorse (DGS-UNMIG)
	DG Sicurezza approvvigionamento, infrastrutture energetiche (DG SAIE)
	DG mercato elettrico, energie rinnovabili, efficienza energetica e nucleare (DGMEEREEN)
AOO_Comicazioni (AOO_COM)	DG Pianificazione, gestione spettro radioelettrico (DG PGSR)
	DG Servizi comunicazione elettronica, radiodiffusione, postali (DG SCERP)
	Istituto superiore comunicazioni, tecnologie informazione (ISCTI)
AOO_Attività territoriali (AOO_AT)	DG Attività territoriali (DG AT), compresi gli Ispettorati Territoriali
AOO_Politiche industriali e Tutela (AOO_PIT)	DG Politica industriale, competitività, PMI (DG PICPMI)
	DG Vigilanza enti, sistema cooperativo, gestioni commissariali (DG VESCGC)
	DG Lotta Contraffazione, UIBM (DG LC-UIBM)
	DG Mercato, concorrenza, consumatore, vigilanza, normativa tecnica (DG MCCVNT)
	DG Incentivi alle imprese (DG IAI)
AOO_Internazionalizzazione (AOO_INT)	DG Politica commerciale internazionale (DG PCI)
	DG Politiche internazionalizzazione, promozione scambi (DG PIPS)

Tabella 2: Elenco AOO

11.3 Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi

-Decreto rinnovo servizio gestione informatica

11.4 Procedura per la protocollazione informatica sul Documentale MISE

-Procedura protocollazione documentale MISE

11.5 Flusso documentale UCB

- Circolare avvio flusso UCB

- All.1 flusso UCB - Vademecum MISE

- All.2 flusso UCB - Elenco delle tipologie documentali

- All. 3 flusso UCB -Protocollo d'intesa MISE-UCB

- All. 4 flusso UCB - Protocollazione automatizzata - specifiche tecniche

11.6 Procedure di gestione di flussi documentali specifiche delle Direzioni Generali

11.7 Titolari d'archivio AOO

11.7.1 Titolare - Area Organizzativa: UFFICI DI DIRETTA COLLABORAZIONE DEL MINISTRO

- Titolare AOO_UDCM

11.7.2 Titolare - Area Organizzativa: AOO_INCENTIVI

- Titolare AOO_IAI

11.7.3 Titolare - Area Organizzativa: AOO_AFFARI GENERALI

- Titolare AOO_AG

11.7.4 Titolare - Area Organizzativa: AOO_ATTIVITA' TERRITORIALI

- Titolare AOO_AT

11.7.5 Titolare - Area Organizzativa: AOO_COMUNICAZIONI

- Titolare AOO_COM

11.7.6 Titolare - Area Organizzativa: AOO_ENERGIA

- Titolare AOO_ENE

11.7.7 Titolare - Area Organizzativa: AOO_INTERNAZIONALIZZAZIONE

- Titolare AOO_INT

11.7.8 Titolare - Area Organizzativa: AOO_POLITICHE INDUSTRIALI E TUTELA

- Titolare AOO_PIT

11.7.9 Schema Titolare

- Indicazioni di fascicolazione-schema Titolare

11.8 Piano di conservazione

11.8.1 Massimario - Area Organizzativa: AOO_AFFARI GENERALI

- Massimario voci 1-9

11.9 Procedura per la Protocollazione in Emergenza

- Manuale protocollo emergenza