

# COMUNE DI POLICORO

## PROVINCIA DI MATERA



# MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO E DELL'ARCHIVIO DEL COMUNE DI POLICORO

Approvato con delibera di G.C. n.102 del 29-07-2015

## Indice

Indice.....	2
1PRINCIPI GENERALI .....	5
1.1Premessa.....	5
1.2Ambito di applicazione del Manuale.....	5
1.3Definizioni e norme di riferimento .....	6
1.4Aree organizzative omogenee e modelli organizzativi.....	6
1.5Servizio per la gestione informatica del protocollo.....	7
1.6Conservazione delle copie di riserva .....	7
1.7Firma digitale .....	7
1.8Tutela dei dati personali .....	7
1.9Caselle di posta elettronica.....	8
1.10Sistema di classificazione dei documenti.....	8
1.11Formazione .....	8
1.12Accreditamento dell'amministrazione / AOO all'IPA .....	9
1.13Procedure integrative di conservazione sostitutiva.....	9
2.ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO .....	9
2.1Piano di attuazione.....	9
3.PIANO DI SICUREZZA .....	10
3.1Obiettivi del piano di sicurezza.....	10
3.2Generalità .....	10
3.3Formazione dei documenti - aspetti di sicurezza .....	11
3.4Gestione dei documenti informatici.....	11
3.5Trasmissione e interscambio dei documenti informatici.....	14
3.6Accesso ai documenti informatici.....	15
3.7Conservazione dei documenti informatici.....	17
3.8Politiche di sicurezza adottate dalla AOO.....	17
4.MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI.....	18
4.1Documento ricevuto.....	18
4.2Documento inviato.....	19
4.3Documento interno formale.....	19
4.4Documento interno informale .....	19
4.5Documento analogico-cartaceo .....	19
4.6Formazione dei documenti - aspetti operativi .....	19
4.7Sottoscrizione di documenti informatici.....	20

4.8	Requisiti degli strumenti informatici di scambio .....	20
4.9	Firma digitale .....	20
4.10	Verifica delle firme nel PdP per i formati .p7m.....	21
4.11	Uso della posta elettronica certificata.....	21
5.	DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI.....	22
5.1	Generalità .....	22
5.2	Flusso dei documenti in ingresso alla aoo .....	22
5.3	Flusso dei documenti in uscita dalla AOO.....	28
6.	REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI .....	30
6.1	Regole disponibili con il PdP.....	30
6.2	Corrispondenza di particolare rilevanza .....	31
6.3	Assegnazione dei documenti ricevuti in formato digitale .....	31
6.4	Assegnazione dei documenti ricevuti in formato cartaceo .....	31
6.5	Modifica delle assegnazioni .....	32
7.	UO RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI.....	32
7.1	Servizio archivistico .....	32
7.2	Servizio della conservazione elettronica dei documenti.....	32
8.	ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE.....	33
8.1	Documenti esclusi.....	33
8.2	Documenti soggetti a registrazione particolare.....	33
9.	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE.....	33
9.1	Protezione e conservazione degli archivi pubblici .....	33
9.2	Titolario o piano di classificazione .....	34
9.3	Fascicoli .....	35
9.4	Serie archivistiche e repertori .....	36
9.5	Consultazione e movimentazione dell'archivio corrente, di deposito e storico.....	38
10.	Modalità di produzione e di conservazione delle registrazioni di protocollo informatico .....	40
10.1	Unicità del Protocollo Informatico.....	40
10.2	Registro giornaliero di protocollo .....	40
10.3	Registrazione di protocollo.....	40
10.4	Elementi facoltativi delle registrazioni di protocollo.....	41
10.5	Segnatura di protocollo dei documenti.....	42
10.6	Annullamento delle registrazioni di protocollo .....	43
10.7	Livello di riservatezza .....	43
10.8	Casi particolari di registrazioni di protocollo.....	43
10.9	Gestione delle registrazioni di protocollo con il PdP.....	46
10.10	Registrazioni di protocollo .....	46

11.DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO .....	47
11.1 Generalità.....	47
11.2 Abilitazioni interne ad accedere ai servizi di protocollo .....	48
12.MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA .....	48
12.1 Il registro di emergenza.....	48
12.2 Modalità di apertura del registro di emergenza .....	48
12.3 Modalità di utilizzo del registro di emergenza .....	49
12.4 Modalità di chiusura e di recupero del registro di emergenza .....	49
13.GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI.....	49
13.1 Matrice delle correlazioni.....	49
13.2 Elenco dei procedimenti amministrativi.....	49
13.3 Avvio dei procedimenti e gestione degli stati di avanzamento .....	50
14. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI.....	50
14.Modalità di approvazione e aggiornamento del manuale .....	50
14.1 Regolamenti abrogati.....	50
14.3 Pubblicità del presente manuale .....	50
14.4 Operatività del presente manuale .....	50
15.ALLEGATI .....	51
15.1 Definizioni .....	51
15.2 Area organizzativa omogenea e modello organizzativo .....	59
15.3 Politiche di sicurezza .....	60
15.4 Regole di gestione della corrispondenza convenzionale in ingresso e in uscita al/dal servizio postale .....	61
15.5 Elenco dei documenti esclusi dalla registrazione di protocollo .....	61
15.6 Elenco dei documenti soggetti a registrazione particolare.....	62
15.7 Titolario di classificazione .....	63

# 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, dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

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

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

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

Esso disciplina:

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

Il Manuale è articolato in due parti, nella prima sono 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 e archiviazione dei documenti, oltre che la gestione dei flussi documentali e archivistici riguardo ai procedimenti amministrativi del COMUNE DI POLICORO.

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

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

### 1.3 Definizioni e norme di riferimento

Ai fini del presente Manuale si intende:

- per "amministrazione", COMUNE DI POLICORO;
- 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 e s.m.i. - Codice dell'amministrazione digitale.

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

- **AOO - Area Organizzativa Omogenea;**
- **MdG - Manuale di Gestione** del protocollo informatico e gestione documentale e degli archivi;
- **RPA - Responsabile del Procedimento Amministrativo** - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi a un affare;
- **RSP - Responsabile del Servizio per la tenuta del Protocollo informatico**, la gestione dei flussi documentali e degli archivi;
- **PdP - Prodotto di Protocollo informatico** - l'applicativo sviluppato o acquisito dall'amministrazione per implementare il servizio di protocollo informatico;
- **UOP - Unità Organizzative di registrazione di Protocollo** - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UO - Uffici Organizzativi** - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU - Ufficio Utente** - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

### 1.4 Aree organizzative omogenee e modelli organizzativi

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata AOO COMUNE DI POLICORO che è composta dall'insieme di tutte le UO e gli UU articolati come riportato nell'allegato 15.2.

All'interno della AOO il sistema di protocollazione è unico.

Nell'AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme delle UO che la compongono con la loro articolazione in U U.

All'interno dell'AOO il sistema di protocollazione è centralizzato per la corrispondenza in ingresso, mentre è decentralizzato, per la corrispondenza in uscita, attraverso tutte le UO.

L'allegato 15.2. è suscettibile di modifica in caso di inserimento di nuove AOO/UO/UU o di riorganizzazione delle medesime.

Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali.

L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UU allo svolgimento dell'attività di protocollazione.

Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del responsabile del protocollo informatico.

Nelle UO sarà utilizzato il medesimo sistema di numerazione di protocollo e gli incaricati dell'attività di

protocollazione dovranno essere abilitati dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

## **1.5 Servizio per la gestione informatica del protocollo**

Nell'AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).

Egli è funzionalmente individuato nel I Settore “ Amministrativo”, alle dirette dipendenze del Responsabile del Settore e può coincidere con il Responsabile dello stesso.

È compito del servizio, in collaborazione, per quanto di competenza, con il SIC,:

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

## **1.6 Conservazione delle copie di riserva**

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della settimana lavorativa, va riversato, nel rispetto della normativa vigente, su supporti informatici non riscrivibili.

Tali supporti rimovibili sono conservati dalla stessa persona che ha realizzato il riversamento.

Le procedure di riversamento e custodia delle copie, predisposte dal RSP, sono illustrate nel piano di sicurezza del MdG.

## **1.7 Firma digitale**

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata a i soggetti da essa delegati a rappresentarla.

## 1.8 Tutela dei dati personali

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

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

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

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

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

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

## 1.9 Caselle di posta elettronica

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

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

## 1.10 Sistema di classificazione dei documenti

Con l'inizio della attività operativa del protocollo unico viene adottato anche un unico- titolare di classificazione dell'amministrazione per l'AOO che identifica l'amministrazione stessa.

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

Il contenuto della classificazione è dettagliatamente illustrato nel successivo Capitolo 9.

## 1.11 Formazione

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

In particolare, considerato che il personale assegnato alle UO deve conoscere sia l'organizzazione ed i compiti svolti da ciascuna UO e da ciascun 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 previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

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

## **1.12 Accredimento dell'amministrazione / AOO all'IPA**

L'amministrazione/ AOO è dotata una casella di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UO incaricata; l'UO 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 dalla DIGIT PA fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;
- l'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 delle UO e degli UU dell'AOO.

Le informazioni inerenti all'amministrazione sono riportate nell'allegato 15.2.

Il codice identificativo della amministrazione associato alla AOO, è stato generato e attribuito autonomamente dall'amministrazione.

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione ovvero la creazione di una AOO.

## **1.13 Procedure integrative di conservazione sostitutiva**

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniformerà alle modalità previste dalla deliberazione CNIPA n. 11/2004 e dalle Regole Tecniche previste dal DPCM del 13/11/2014 nei tempi dagli stessi previsti. Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunica alla DIGIT PA le procedure integrative che intende adottare ai sensi dell'art. 7 della citata deliberazione.

# **2. ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO**

## **2.1 Piano di attuazione**

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione

sono registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati.

Il RSP esegue comunque, periodicamente, dei controlli a campione sul corretto e regolare utilizzo di un unico registro di protocollo, verificando, attraverso controlli e ispezioni mirate nelle varie UO/UU, la validità dei criteri di classificazione utilizzati.

## **3. PIANO DI SICUREZZA**

### **3.1 Obiettivi del piano di sicurezza**

Il piano di sicurezza garantisce che:

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

### **3.2 Generalità**

Il responsabile del sistema informativo ha predisposto il piano di sicurezza.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

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

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.

Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/ AOO;
- protezione dei sistemi di 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 bimestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura del Servizio Informatico delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e

- service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

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

### 3.3 Formazione dei documenti - aspetti di sicurezza

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

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

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, ODF, XML

I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e ODF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici) e dal DPCM del 13/11/2014.

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 a un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione / AOO.

### 3.4 Gestione dei documenti informatici

Il sistema operativo del PdP utilizzato dall'amministrazione/ AOO, è conforme alle specifiche previste

dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

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

Il sistema di gestione informatica dei documenti:

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

### **Componente organizzativa della sicurezza**

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/ AOO.

Nella conduzione del servizio destinato ad erogare il PdP, le qualifiche funzionali individuate sono le seguenti:

- responsabile della sicurezza;
- responsabile della tutela dei dati personali;
- responsabile dei sistemi e delle reti;
- operatore (sistemi e TLC).

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

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

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

- responsabile della sicurezza;
- responsabile CED;
- operatori della sicurezza.

La componente organizzativa della sicurezza afferente l'AOO è articolata e gestita secondo quanto stabilito dal I Settore dell'Ente.

### **Componente fisica della sicurezza**

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato

secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti non possono entrare e trattenersi nelle aree protette se non accompagnati da personale interno autorizzato a quel livello di protezione;
- il personale della sede ha l'obbligo di utilizzare il badge sia in ingresso che in uscita dalla sede stessa.

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

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

Il controllo degli accessi fisici alle risorse della sede dell'amministrazione/ AOO è regolato secondo i principi stabiliti dal I Settore.

### **Componente logica della sicurezza**

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

Tale componente, nell'ambito del PdP, è stata realizzata attraverso:

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

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle best practices correnti.

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti dell'AOO e degli operatori dell'erogatore del PdP, con le seguenti caratteristiche:

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

### **Componente infrastrutturale della sicurezza**

Essendo il CED lontano da insediamenti industriali e posto all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

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

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

### **Gestione delle registrazioni di protocollo e di sicurezza**

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

Le registrazioni di sicurezza sono costituite:

- dai log di sistema, generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system- IDS, sensori di rete e firewall);
- dalle registrazioni dell'applicativo PdP.

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

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

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

### **3.5 Trasmissione e interscambio dei documenti informatici**

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider ) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del

- messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

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

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

### **All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)**

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MI ME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

### **All'interno della AOO**

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

Gli Uffici dell'amministrazione (UO/ UU) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica (eventualmente certificata ai sensi del decreto del Presidente della Repubblica n. 68 dell'11 febbraio 2005) in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l'"impiego della posta elettronica nelle pubbliche amministrazioni".

## **3.6 Accesso ai documenti informatici**

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Queste, in sintesi, sono:

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

Le regole per la composizione delle password e per il blocco delle utenze valgono sia per l'amministratore della che per gli utenti della AOO.

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

Il PdP adottato dall'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.

Ad ogni registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il PdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua UO, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

### **Utenti interni alla AOO**

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

La gestione delle utenze rispetta i seguenti criteri operativi:

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

### **Accesso al registro di protocollo per utenti interni alla AOO**

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

- ruoli degli utenti, gestiti dall'amministratore di ente (amministrazione), per la specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "particolare o riservata", gestita dall'amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. Tale vista è definita dalle voci di titolare associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).

L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo ed assegnarlo per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e ai protocollatori che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).

Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo del protocollo (ad esempio: classificazione).

### **Utenti esterni alla AOO - altre amministrazioni**

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre

amministrazioni avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le amministrazioni che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'UU di appartenenza del RPA.

### **Utenti esterni alla AOO - privati**

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

## **3.7 Conservazione dei documenti informatici**

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

### **SERVIZIO ARCHIVISTICO**

Il responsabile del sistema archivistico dell'intera amministrazione, che coincide con il RSP, ha individuato nei locali al piano seminterrato e negli armadi ubicati nei corridoi e nelle stanze della sede istituzionale dell'amministrazione medesima, la sede del relativo archivio dell'amministrazione.

Il responsabile del servizio in argomento ha effettuato la scelta alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti.

Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha, in corso di perfezionamento, un piano specifico individuando, i soggetti incaricati di ciascuna fase.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità, nel tempo, di tutti i documenti trasmessi o ricevuti, adottando i formati previsti dalle regole tecniche vigenti.

### **Servizio di conservazione sostitutiva**

Il servizio è attualmente in fase di definizione.

### **Conservazione dei documenti informatici e delle registrazioni di protocollo**

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

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

### **Riutilizzo e dismissione dei supporti rimovibili**

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

## **3.8 Politiche di sicurezza adottate dalla AOO**

Le politiche di sicurezza, riportate nell'allegato 15.3, stabiliscono, sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure consuntive per la gestione degli incidenti informatici.

È compito del responsabile della sicurezza e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza

complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste.  
In ogni caso, tale attività è svolta almeno con cadenza annuale.

## **4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI**

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

Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo. Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è così classificabile:

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

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

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e "2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità".

Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

L'Amministrazione comunale procederà ad adottare tutte le misure stabilite dal Decreto....., per la formazione, conservazione ed archiviazione dei documenti informatici nel termine dallo stesso previste.

### **4.1 Documento ricevuto**

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

Un documento informatico può essere recapitato:

- a mezzo posta elettronica convenzionale o certificata;
- su supporto rimovibile quale, ad esempio, cd rom, dvd, floppy disk, tape, pen drive, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telefax o telegramma;
- con consegna diretta da parte dell'interessato tramite una persona dallo stesso delegata alle UO e/o agli UU aperti al pubblico.

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

## 4.2 Documento inviato

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista, dal sistema di posta utilizzato dall'AOO e con un limite congruo di destinatari.

In caso contrario, il documento informatico viene copiato, su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi di trasporto.

## 4.3 Documento interno formale

I documenti interni sono formati con tecnologie informatiche .

Lo scambio tra UO/ UU di documenti informatici di rilevanza amministrativa giuridico-probatoria, avviene di norma per mezzo della posta elettronica convenzionale, o, se disponibile, di quella certificata.

Il documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato.

Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa e successivamente protocollato.

## 4.4 Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

## 4.5 Documento analogico-cartaceo

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

In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa. Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del manuale.

## 4.6 Formazione dei documenti - aspetti operativi

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

Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

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

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

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dal responsabile delle singole UO.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e della UO e dell'UU che ha prodotto il documento;

- l'indirizzo completo dell'amministrazione (via, numero civico, CAP, città, provincia);
- il numero di telefono dell'UU;
- il numero di fax della UO;
- il codice fiscale dell'amministrazione;
- l'indirizzo del portale istituzionale;
- l'indirizzo di posta istituzionale e della posta elettronica certificata istituzionale.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione<sup>1</sup>;
- la data (giorno, mese, anno);
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto;
- firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale; se trattasi di documento digitale;
- sigla autografa dell'istruttore e sottoscrizione autografa del responsabile del procedimento amministrativo (RPA) e/o del responsabile del provvedimento finale, se trattasi di documento cartaceo.

#### **4.7 Sottoscrizione di documenti informatici**

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

I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi art 3, comma 3, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

L'Amministrazione Comunale provvederà ad adeguare la formazione, trasmissione e conservazione dei documenti informatici nei tempi e con le modalità previste dal DPCM 13/11/2014.

#### **4.8 Requisiti degli strumenti informatici di scambio**

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

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

#### **4.9 Firma digitale**

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.8 è la firma digitale utilizzata per inviare e ricevere documenti per l'AOO per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro file digitale con valenza giuridico-probatoria.

---

<sup>1</sup> Questo valore è riportato all'interno dell'etichetta di segnatura del protocollo.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza con modalità conformi a quanto prescritto dalla normativa vigente in materia.

#### **4.10 Verifica delle firme nel PdP per i formati .p7m**

Nel PdP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

La sequenza delle operazioni previste è la seguente:

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato; questa attività è realizzata verificando on-line le Certificate Revocation List (CRL) con una periodicità predefinita parametricamente. Una giacenza in memoria temporanea (cache) di un'ora è considerata accettabile;
- verifica della firma (o delle firme multiple) con funzioni java standard; in particolare, viene calcolata l'impronta del documento e verificata con quella contenuta nella busta "logica";
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate presso DigitPA con periodicità settimanale;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF o XML o TIFF) e attribuzione della segnatura di protocollo;
- inserimento nel sistema documentale del PdP sia del documento originale firmato, sia del documento in chiaro;
- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del PdP per accelerare successive attività di verifica di altri documenti ricevuti.

E' in corso l'aggiornamento del PdP ai suddetti standard.

#### **4.11 Uso della posta elettronica certificata**

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici). Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica); firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della posta elettronica certificata (PEC) consente di:

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

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

I messaggi di ritorno, che sono classificati in:

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

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica amministrazione (IPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa, vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

## **5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI**

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

L'UOP non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

### **5.1 Generalità**

Per descrivere i flussi di lavorazione dei documenti all'interno dell'AOO si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.

Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;

inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/ AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.

### **5.2 Flusso dei documenti in ingresso alla aoo**

## PROTOCOLLO INFORMATICO - Flusso dei documenti in ingresso alla AOO

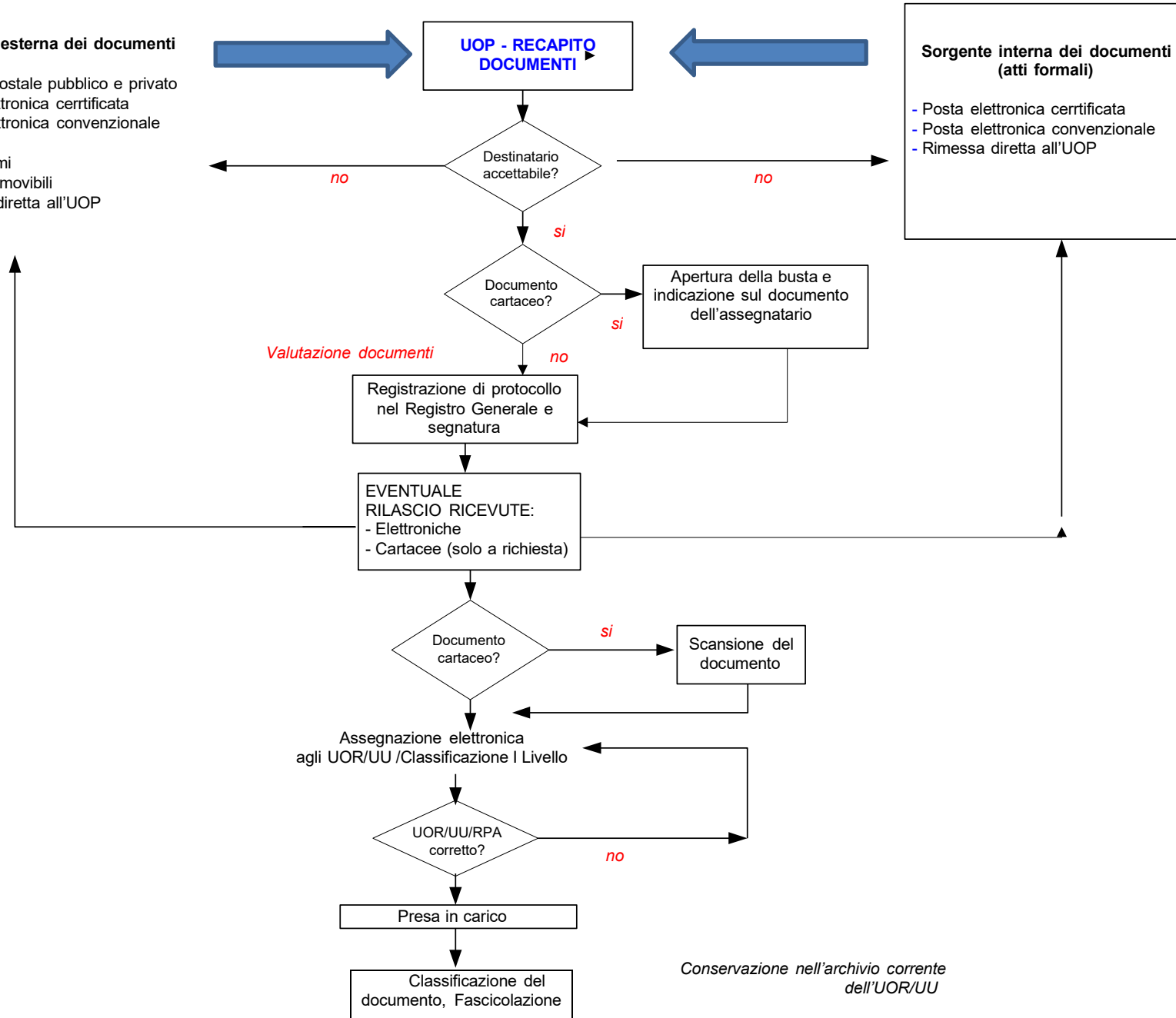
### Sorgente esterna dei documenti

- Servizio postale pubblico e privato
- Posta elettronica certificata
- Posta elettronica convenzionale
- Fax
- Telegrammi
- Supporti rimovibili
- Rimessa diretta all'UOP

### UOP - RECAPITO DOCUMENTI

### Sorgente interna dei documenti (atti formali)

- Posta elettronica certificata
- Posta elettronica convenzionale
- Rimessa diretta all'UOP



### **Provenienza esterna dei documenti**

I documenti trasmessi da soggetti esterni all'AOO sono, oltre a quelli richiamati nel capitolo precedente, i telefax, i telegrammi ed eventuali supporti digitali rimovibili allegati a documenti cartacei. Questi documenti sono recapitati alla UOP.

Ci sono apparati fax dislocati in diversi UU. I fax pervenuti sono inviati alla UO per la protocollazione.

I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente alla UOP in parola, che si fa carico di selezionare e smistare la corrispondenza.

### **Provenienza di documenti interni formali**

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

Il documento è, di norma, di tipo analogico secondo i formati standard illustrati nel precedente capitolo. In questo caso, il mezzo di recapito della corrispondenza considerato è la posta interna.

### **Ricezione di documenti informatici sulla casella di posta istituzionale**

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla UOP dell'AOO e tramite le altre caselle di PEC assegnate ad altri uffici, che provvederanno allo scarico delle stesse, mentre la protocollazione rimane assegnata alla UOP dell'AOO.

Quando i documenti informatici pervengono alla UO, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo ed alla assegnazione agli UU di competenza.

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

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

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

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

Il personale della UOP controlla quotidianamente i messaggi pervenuti nelle caselle di posta istituzionale e verifica se sono da protocollare.

I messaggi possono pervenire altresì alla casella di posta elettronica istituzionale ( [posta@policoro.gov.it](mailto:posta@policoro.gov.it) ) e se aderenti alle regole tecniche in vigore, protocollati e assegnati all'UU. In questo caso, dato che il sistema non permette l'automazione del flusso documentale, possono essere inoltrati via posta elettronica all'ufficio destinatario.

### **Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale**

Nel caso in cui il messaggio è ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio stesso viene inoltrato alla casella di posta istituzionale. I controlli effettuati sul messaggio sono quelli sopra richiamati.

Alla stessa maniera la UOP provvede alla protocollazione ed assegnazione dei messaggi pervenuti dagli indirizzi di posta elettronica istituzionali o personali inoltrati dagli UU.

### **Ricezione di documenti informatici su supporti rimovibili**

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

Nei casi in cui un documento è cartaceo mentre gli allegati sono trasmessi su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di /i/e digitali, la AOO si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti del caso.

L'acquisizione degli allegati digitali nel sistema PdP può avvenire solo se la grandezza totale di ogni allegato non supera il limite di 5 Megabyte.

Gli allegati che superano tale dimensione dovranno essere riversati su un apposito disco virtuale condiviso e visibile dagli utenti assegnatari.

### **Ricezione di documenti cartacei a mezzo posta convenzionale**

I documenti pervenuti a mezzo posta sono consegnati alla UOP.

Le buste, o contenitori, sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario apposti sugli stessi.

La corrispondenza relativa a bandi di gara non viene aperta, ma, dopo essere stata esaminata dal personale dell'Ufficio "Amministrazione gare e contratti", che appone sulla busta la data e l'ora di arrivo della busta medesima, viene registrata al protocollo con la segnatura applicata sull'esterno del plico e successivamente riconsegnata chiusa all'Ufficio competente.

La corrispondenza personale non è aperta, né protocollata, ma viene consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'Ufficio protocollo per la registrazione.

La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo con le modalità descritte nel successivo capitolo 11. Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

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

### **Errata ricezione di documenti digitali**

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

### **Errata ricezione di documenti cartacei**

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

### **Attività di protocollazione dei documenti**

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

### **Rilascio di ricevute attestanti la ricezione di documenti informatici**

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

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

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

### **Rilascio di ricevute attestanti la ricezione di documenti cartacei**

Gli addetti alle UO di protocollazione non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

La semplice apposizione del timbro datario della UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale della UO in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente dal mittente, o da altra persona incaricata alla UOP, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP è autorizzata a:

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

Nel caso di corrispondenza pervenuta ad una UO o ad un UU, questa deve consegnarla alla UOP allo scopo di ottenere una ricevuta valida.

### **Conservazione dei documenti informatici**

I documenti informatici sono archiviati sui supporti di memorizzazione del CED, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

I documenti ricevuti per via telematica sono resi disponibili alle UO/UU, attraverso la rete interna dell'amministrazione subito dopo l'operazione di assegnazione.

### **Conservazione delle rappresentazioni digitali di documenti cartacei**

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione che avviene secondo le fasi di seguito indicate:

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

Nel caso in cui, per le particolari caratteristiche di formato (progetti ed elaborati grafici, etc.) non sia possibile procedere con i mezzi tecnici in dotazione all'AOO, all'acquisizione digitale dei documenti, viene acquisita digitalmente esclusivamente la lettera di trasmissione e il cartaceo viene smistato all'ufficio di destinazione.

Le rappresentazioni digitali dei documenti cartacei sono archiviate sui sistemi del CED, secondo le regole vigenti, su supporti di memorizzazione, in modo non modificabile al termine del processo di scansione.

I documenti cartacei dopo l'operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della deliberazione CNIPA 19 febbraio 2004, n. 11 vengono trattati diversamente in base alla loro tipologia.

Gli originali dei documenti cartacei ricevuti, di norma non vengono inviati alle UO ma rimangono e vengono archiviati in ordine sequenziale di protocollo dalla UOP.

A questa regola fanno eccezione i documenti seguenti:

- richieste di parere (inviati all'ufficio competente);
- corrispondenza riguardante il personale dipendente;
- originale delle lettere-contratto firmate per accettazione;
- originale delle fatture e documentazione contabile da esibire per eventuali controlli, fermo restando le specifiche disposizioni in materia di fatturazione elettronica.

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

### **Assegnazione, presa in carico dei documenti e classificazione.**

Gli addetti alla UOP provvedono a:

- eseguire la prima classificazione e/o classificazione di primo livello del documento sulla base del titolare di classificazione in essere presso l'AOO, solo in assenza del meccanismo di assegnazione e classificazione automatica predisposto nel PdP;
- inviare il documento all'UO che identifica l'UU di destinazione.

La UO:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP mittente;
- in caso di verifica positiva, esegue l'operazione di presa in carico riassegnandola al proprio interno ad un UU o direttamente al RPA;

### **Conservazione dei documenti nell'archivio corrente**

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

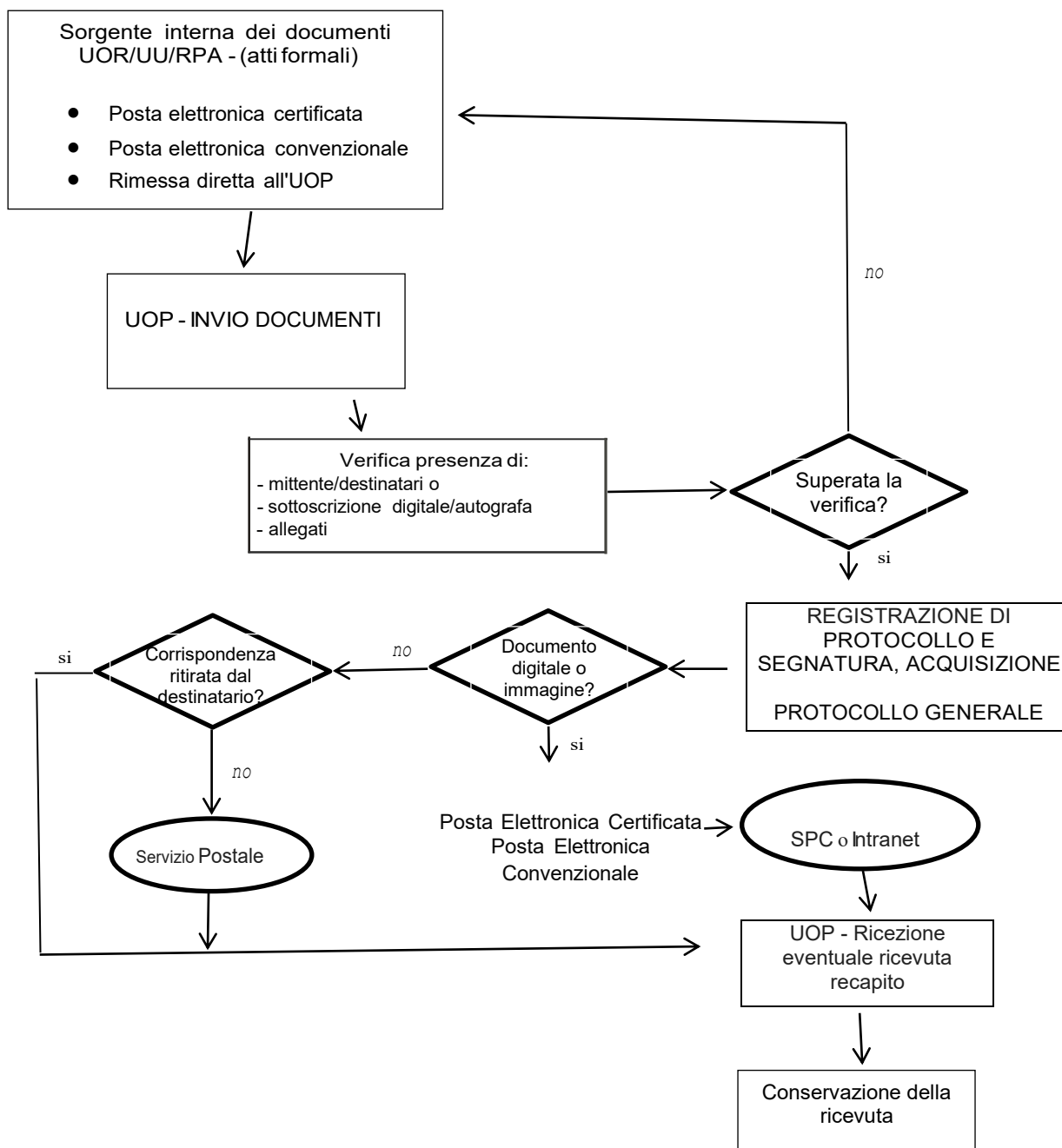
- classificazione di livello superiore sulla base del titolare di classificazione adottato dall'AOO;
- fascicolazione del documento secondo le procedure previste dall'AOO;
- inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

### **Conservazione dei documenti e dei fascicoli nella fase corrente**

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

## 5.3 Flusso dei documenti in uscita dalla AOO

### PROTOCOLLO INFORMATICO - Flusso dei documenti in uscita dalla AOO



#### Sorgente interna dei documenti

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

Per "documenti in uscita" s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio

delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione.

Per "documenti in uscita" si possono intendere anche quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altro ufficio (UU) della stessa AOO.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti capitoli. I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nel paragrafo 4.11 - Uso della posta elettronica certificata.

Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.

I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.

Durante la fase transitoria di migrazione all'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo caso sono il servizio postale, nelle sue diverse forme, ed il servizio telefax.

### **Verifica formale dei documenti**

Ogni UU è autorizzata dall'AOO per il tramite del RSP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.

Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati dagli UU e spediti dal UOP.

Gli UU provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

Se la verifica da esito positivo, il documento è registrato nel registro di protocollo generale; in caso contrario è restituito al mittente UU/RPA con le osservazioni del caso.

### **Registrazione di protocollo e segnatura**

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UU abilitati in quanto collegati al sistema di protocollo informatico della AOO.

Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA. Il documento registrato presso il protocollo riservato è contrassegnato antepponendo al numero della segnatura una sigla.

### **Trasmissione di documenti informatici**

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AIPA 7 maggio 2001, n. 28.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).

Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale propri di certificatore accreditato iscritto nell'elenco pubblico tenuto dal CNIPA.

Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via

telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

### **Trasmissione di documenti cartacei a mezzo Posta elettronica / PEC**

Gli UU possono provvedere alla trasmissione mediante posta elettronica certificata o posta elettronica di documenti cartacei, previa acquisizione digitale dell'immagine degli stessi con l'indicazione della segnatura di protocollo.

### **Trasmissione di documenti cartacei a mezzo posta**

Gli UU provvedono alla trasmissione "fisica" del documento in partenza, di norma il giorno lavorativo in cui è stato protocollato.

### **Affrancatura dei documenti in partenza**

L'UOP provvede alle operazioni necessarie per l'invio della corrispondenza in partenza (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.).

Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP, di norma, entro le ore 11:30.

La corrispondenza consegnata oltre il termine sopraindicato sarà spedita il giorno lavorativo successivo.

### **Conteggi spedizione corrispondenza**

L'UOP effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

### **Trasmissione di documenti cartacei a mezzo telefax**

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

Le ricevute dell'avvenuta trasmissione sono trattenute dagli UU che hanno inviato il fax.

### **Inserimento delle ricevute di trasmissione nel fascicolo**

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

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

## **6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI**

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

### **6.1 Regole disponibili con il PdP**

L'assegnazione dei documenti protocollati e segnati avviene sfruttando le funzionalità di seguito descritte.

Il PdP, per abbreviare il processo di assegnazione del materiale documentario oggetto di lavorazione, utilizza l'organigramma dell'AOO.

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

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

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

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

## **6.2 Corrispondenza di particolare rilevanza**

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

## **6.3 Assegnazione dei documenti ricevuti in formato digitale**

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UO competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile interni al centro servizio.

L'UO competente ha notizia dell'assegnazione di detti documenti tramite un messaggio di posta elettronica di notifica di assegnazione.

Il responsabile dell'UO è in grado di visualizzare i documenti, attraverso le funzionalità del PdP e, in base alle abilitazioni possedute, potrà:

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

La "presa in carico" dei documenti informatici è registrata dal PdP in modo automatico e la data di ingresso dei documenti nelle UO competenti coincide con la data di assegnazione degli stessi.

I destinatari del documento lo ricevono esclusivamente in formato digitale.

## **6.4 Assegnazione dei documenti ricevuti in formato cartaceo**

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

Il responsabile dell'UO può visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente sulla materia oggetto del documento.

La "presa in carico" dei documenti informatici è registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UO di competenza coincide con la data di assegnazione degli stessi.

Il ritiro giornaliero della corrispondenza cartacea in arrivo da parte dalle UO/UU/RPA avviene presso la UOP ricevente.

## **6.5 Modifica delle assegnazioni**

Nel caso di assegnazione errata, l'UO/UU che riceve il documento comunica l'errore alla UOP, che procederà ad una nuova assegnazione.

Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenze attribuite ad altro UU della stessa UO, l'abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UO medesima, o a persona da questi incaricata.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data di esecuzione.

## **7. UO RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI**

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

In base al modello organizzativo adottato dall'Amministrazione/ AOO (si veda il par. 1.4 del presente MdG), nell'allegato 15.2 è riportato, per ciascuna AOO, l'elenco delle unità organizzative responsabili delle attività di registrazione del protocollo (UOP).

### **7.1 Servizio archivistico**

Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto servizio per la tenuta del protocollo informatico.

### **7.2 Servizio della conservazione elettronica dei documenti**

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

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

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

Il ruolo di pubblico ufficiale per la chiusura dei supporti rimovibili è svolto dal dirigente dell'ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per i casi nei quali si richiede l'intervento di soggetto diverso nel rispetto delle disposizioni di normative e delle regole tecniche.

#### **Archiviazione ottica dei documenti analogici**

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

#### **Archiviazione ottica dei documenti digitali**

Il processo di conservazione sostitutiva dei documenti informatici, anche sottoscritti, inizia con la memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento

temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento di tale processo.

Il processo di riversamento sostitutivo di documenti informatici avviene mediante memorizzazione su altro supporto ottico e termina con l'apposizione sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.

Qualora il processo riguardi documenti informatici sottoscritti è richiesta anche l'apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d'origine.

## **8. ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE.**

### **8.1 Documenti esclusi**

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 come riportato nell'allegato 15.5.

### **8.2 Documenti soggetti a registrazione particolare**

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'allegato 15.6.

Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.

Questi documenti costituiscono comunque delle serie di interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

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

## **9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE**

### **9.1 Protezione e conservazione degli archivi pubblici**

#### **Generalità**

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

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

Il titolario e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli

strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione.

Il titolare e il piano di conservazione sono adottati dall'amministrazione con atti formali.

### **Misure di protezione e conservazione degli archivi pubblici**

Gli archivi e i singoli documenti dello Stato, delle regioni e degli enti pubblici sono beni culturali inalienabili.

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

L'archivio non può essere smembrato e deve essere conservato nella sua organicità.

L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.

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

Lo scarto dei documenti dell'archivio in parola è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza a livello provinciale o delle commissioni di scarto istituite presso ogni ufficio con competenza "subprovinciale".

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

## **9.2 Titolare o piano di classificazione**

### **Titolario**

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il piano di classificazione di riferimento si suddivide in titoli e classi o, più in generale, in voci di I livello e II livello.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); la successiva partizione, classi, corrisponde a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli e classi sono nel numero prestabilito dal titolare di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della Giunta Comunale.

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

L'aggiornamento del titolare compete esclusivamente alla Giunta Comunale, su proposta del RSP. La revisione, anche parziale, del titolare viene proposta dal RSP quando necessario ed opportuno.

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

Il titolare non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di titolare e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolare vigente al momento della produzione degli stessi.

Per ogni specifica voce è riportata la data di inserimento e la data di variazione.

Di norma le variazioni sono introdotte dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo titolare e hanno durata almeno per l'intero anno.

Rimane possibile, se il sistema lo consente, di registrare documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi.

## **Classificazione dei documenti**

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dalle UO dell'AOO, indipendentemente dal supporto sul quale sono formati, sono classificati in base al sopra citato titolario.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe), il numero del fascicolo.

Le operazioni di classificazione sono svolte in una prima fase dall'UOP e completate dalle UO/UU destinatari/istruttori di atti.

## **9.3 Fascicoli**

### **Fascicolazione dei documenti**

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

Ogni documento, dopo la classificazione, è inserito nel fascicolo di riferimento.

I documenti sono archiviati all'interno di ciascun fascicolo, secondo l'ordine cronologico di registrazione.

### **Apertura del fascicolo**

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, il RPA provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

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

Il fascicolo è aperto all'ultimo livello della struttura gerarchica del titolario.

### **Chiusura del fascicolo**

Il fascicolo è chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Esso è archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo precedente, primo capoverso, il quale è tenuto pertanto all'aggiornamento del repertorio dei fascicoli.

### **Processo di assegnazione dei fascicoli**

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

Si procede come segue:

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

### **Modifica dell'assegnazione dei fascicoli**

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

### **Repertorio dei fascicoli**

I fascicoli sono annotati nel repertorio dei fascicoli.

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

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

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

Il repertorio dei fascicoli è costantemente aggiornato. Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe, etc.);
- il numero di fascicolo;
- la data di chiusura;
- l'oggetto del fascicolo;
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

## **9.4 Serie archivistiche e repertori**

### **Serie archivistiche**

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

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

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

### **Repertori e serie archivistiche**

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

Con riguardo alla gestione dei documenti cartacei, è previsto che per ogni verbale, delibera, determinazione, decreto, ordinanza e contratto sia, di norma, prodotto un solo originale che viene inserito nel registro di repertorio con il numero progressivo di repertorio;

Una copia conforme all'originale viene conservata nel relativo fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo. Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato al:

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

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

Il repertorio è costantemente aggiornato.

All'interno dell'amministrazione sono istituiti i repertori generali indicati nell'allegato 15.8.

### **Versamento dei fascicoli nell'archivio di deposito**

La formazione dei fascicoli, delle serie e dei repertori è una funzione fondamentale della gestione archivistica.

Periodicamente, e comunque almeno una volta all'anno, il RSP provvede a trasferire i fascicoli e le serie documentarie relativi ai procedimenti conclusi in un'apposita sezione di deposito dell'archivio generale costituito presso l'amministrazione/ AOO.

Per una regolare e costante "alimentazione" dell'archivio di deposito lo stesso responsabile dell'archivio (che può coincidere con il RSP) stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi UU dell'amministrazione/ AOO all'archivio di deposito.

Con la stessa metodologia sono riversati nell'archivio di deposito anche gli altri repertori generali.

La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.

Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Prima di eseguire il conferimento di cui sopra, il RPA/UU procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- della corretta indicazione della data di chiusura sulla camicia del fascicolo;

Il RPA/UU provvede inoltre:

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

Ricevuti i fascicoli e controllato l'aggiornamento del relativo repertorio, il RSP predisponde un elenco di "versamento" da inviare al servizio archivistico.

Copia di detto elenco è conservata dal responsabile che ha versato la documentazione.

I fascicoli che riguardano il personale devono essere trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio.

## **9.5 Consultazione e movimentazione dell'archivio corrente, di deposito e storico**

### **Principi generali**

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

### **Consultazione al fini giuridico- amministrativi**

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 e successive modifiche ed **integrazioni**, dal D.P.R. n. 184 del 12.04.200 e dal regolamento comunale.

### **Consultazione da parte di personale esterno all'Amministrazione**

La domanda di accesso ai documenti è presentata/inviata alla UOP, che provvede a smistarla al servizio archivistico.

Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.

In tal caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico.

La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

### **Consultazione da parte di personale interno all'Amministrazione**

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

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito, o storico, a un ufficio del medesimo UU, od altro UU, avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa, redatta in duplice copia, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UO/UU e la sua firma.

Una copia della richiesta di consultazione è conservata all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione è registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata.

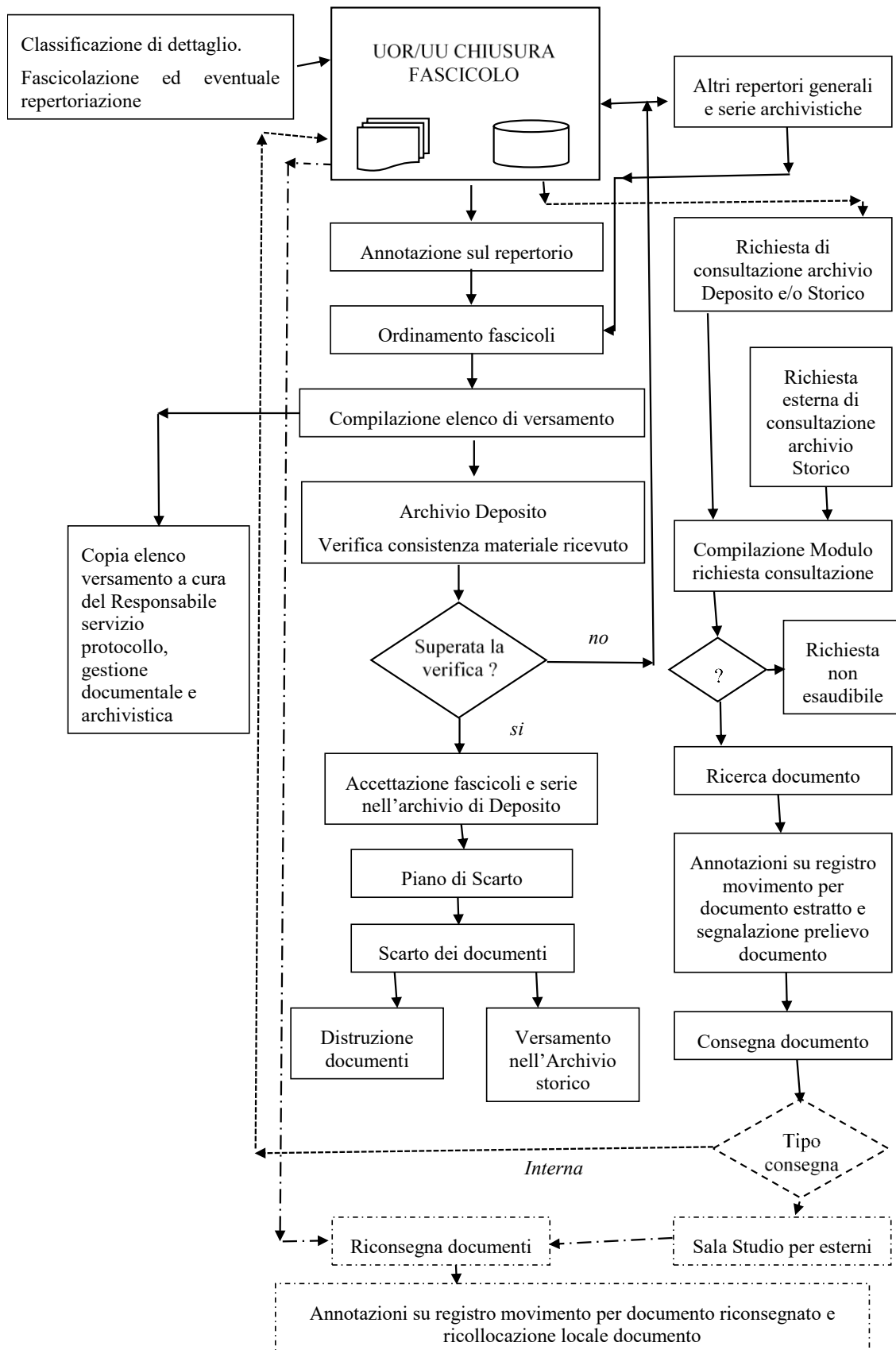
Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine degli stessi rispettandone la sedimentazione archivistica e il vincolo.

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

In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

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



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

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

### 10.1 Unicità del Protocollo Informatico

Nell'ambito dell'AOO il registro generale di protocollo è unico al pari della numerazione progressiva delle registrazioni di protocollo.

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

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

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

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

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

La documentazione che non è stata registrata presso una UO 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 dello stesso, ed è idoneo a produrre effetti giuridici.

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

### 10.2 Registro giornaliero di protocollo

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

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili, i quali sono conservati in luogo sicuro a cura di un soggetto diverso, ai sensi dell'art.7. comma 5, del DPCM 31 ottobre 2000, dal RSP e nominato dall'AOO.

Tale operazione è espletata all'interno del SIC.

### 10.3 Registrazione di protocollo

Di seguito sono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi e interni formali, digitali o analogici).

Su ogni documento ricevuto, o spedito, dall'AOO è eseguita una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori. Tale registrazione è eseguita in un'unica operazione, senza possibilità, per l'operatore, di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

- il mittente che ha prodotto il documento;
- il destinatario o i destinatari del documento;
- l'oggetto del documento;

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

Tali dati facoltativi sono descritti nei paragrafi seguenti.

### **Documenti informatici**

I documenti informatici sono ricevuti, e trasmessi, in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'AOO.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.

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

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere a ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio sia a uno dei file a esso allegati che può assumere la veste di documento principale.

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

La UOP riceve i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

### **Documenti analogici (Cartacei e supporti removibili )**

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento cartaceo ricevuto, così come illustrato nel seguito, è sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

## **10.4 Elementi facoltativi delle registrazioni di protocollo**

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo richiamati nella circolare AI PA 7 maggio 2001 n. 28.

La registrazione degli elementi facoltativi del protocollo, può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UU.

In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

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

- ora e minuto di registrazione;
- mezzo di ricezione /spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- collegamenti a documenti precedenti;
- l'indirizzo completo del mittente/destinatario (via, numero civico, CAP, città, provincia, stato civile, sesso);
- UO/UU competente;
- Il codice fiscale e il numero della partita IVA, il recapito telefonico, il recapito telefax, gli indirizzi di posta elettronica del mittente/destinatario.

## 10.5 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo inequivocabile.

### Documenti informatici

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

Le informazioni minime incluse nella segnatura sono le seguenti:

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

E' facoltativo riportare le seguenti informazioni:

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

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

- persona, ufficio destinatario;
- individuazione degli allegati;
- informazioni sul procedimento e sul trattamento.

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

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

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

### Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione di un'etichetta sulla quale sono riportate le seguenti informazioni riguardanti la registrazione di protocollo:

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

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

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

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

## **10.6 Annullamento delle registrazioni di protocollo**

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Le informazioni riguardanti la 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 e il soggetto che è intervenuto.

Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.

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

## **10.7 Livello di riservatezza**

Il PdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.

Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale.

In modo analogo, il RPA che esegue l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.

Il livello di riservatezza applicato a un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti invece che hanno un livello di riservatezza superiore lo mantengono.

## **10.8 Casi particolari di registrazioni di protocollo**

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

### **Registrazioni di protocollo particolari (riservati)**

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

- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente richiamati nell'allegato 15.6.

### **Circolari e disposizioni generali**

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale. La gestione dei destinatari da associare alla registrazione di protocollo avviene secondo le modalità previste dalla gestione anagrafica del sistema.

### **Documenti cartacei in partenza con più destinatari**

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale.

### **Documenti cartacei ricevuti a mezzo telegramma**

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

### **Documenti cartacei ricevuti a mezzo telefax**

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

All'interno dell'AOO i documenti possono essere anche inviati e ricevuti direttamente dagli UU; per i fax ricevuti, questi ultimi hanno il compito di consegnarli alla UOP per le operazioni di protocollazione. Il documento da chiunque trasmesso all'AOO tramite telefax, qualora ne sia accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.

Nel caso che al telefax faccia seguito l'originale, poiché ogni documento è individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "Già pervenuto via fax il giorno .....".

Il documento in uscita reca una delle seguenti diciture:

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

La segnatura viene apposta sul documento e non sulla copertina di trasmissione del fax.

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

### **Protocollazione di un numero consistente di documenti cartacei**

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

### **Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio**

La corrispondenza ricevuta con rimessa diretta dall'interessato, o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.

Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, gli stessi saranno accantonati e protocollati dopo. In questo caso al mittente, o al suo delegato, è rilasciata ugualmente ricevuta senza gli estremi del protocollo.

### **Fatture, assegni e altri valori di debito o credito**

Le fatture sono protocollate secondo le disposizioni vigenti in materia di fatturazione elettronica. Le fatture escluse dalla predetta normativa, gli assegni o altri valori di debito o credito sono protocollate sul registro ufficiale di protocollo e inviate quotidianamente, in originale, alla UO competente.

### **Protocollo di documenti inerenti gare di appalto confezionate su supporti cartacei**

La corrispondenza che riporta l'indicazione "affetta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione a una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UO competente.

È compito dello stesso UO provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

Per motivi organizzativi tutte le UO sono tenute a informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

### **Protocollo urgenti**

La richiesta di protocollare urgentemente un documento è collegata a una necessità indifferibile e di tipo straordinario.

Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale, o cartaceo, da spedire.

Tale procedura è osservata sia per i documenti in ingresso che per quelli in uscita.

### **Documenti non firmati**

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo" e "documento non sottoscritto".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e sono identificate come tali.

È poi compito dell'UO di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

### **Protocollazione dei messaggi di posta elettronica convenzionale**

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

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

### **Protocollazione di documenti digitali pervenuti erroneamente**

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

### **Ricezione di documenti cartacei pervenuti erroneamente**

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

## **Copie per "CONOSCENZA"**

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

## **Differimento delle registrazioni**

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

Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.

Il protocollo differito consiste nel rinvio dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

## **Corrispondenza personale o riservata**

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

## **Integrazioni documentarie**

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento e gli eventuali allegati. Tale verifica spetta al responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti a integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel relativo fascicolo.

## **10.9 Gestione delle registrazioni di protocollo con il PdP**

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

Il sistema di sicurezza del CED garantisce la protezione di tali informazioni sulla base delle relative architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

## **10.10 Registrazioni di protocollo**

### **Attribuzione del protocollo**

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il PdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente.

Il PdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

Come previsto dalla vigente normativa in materia di protezione dei dati personali l'AOO aderente al PdP è informata della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

### **Registro informatico di protocollo**

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale

dell'AOO, il PdP provvede, in fase di chiusura dell'attività di protocollo, a effettuare le seguenti operazioni:

- estrazione delle registrazioni del giorno corrente dal file del registro generale di protocollo;
- applicazione della firma digitale e di un riferimento temporale al file così realizzato;
- copia del file estratto, del file di firma e del riferimento temporale su supporto rimovibile non riscrivibile;
- salvataggio del file di firma e del riferimento temporale sul sistema di esercizio del PdP.

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

E' inoltre disponibile per le UOP del PdP una funzione applicativa di "Stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

Al termine delle operazioni giornaliere o comunque entro il successivo giorno lavorativo, all'interno del centro servizi dell'erogatore del PdP sono effettuate le seguenti operazioni di garanzia:

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

### **Tenuta delle copie del registro di protocollo**

Il CED provvede con periodicità giornaliera, alla memorizzazione su supporto ottico o magnetico separato, in duplice copia, dei seguenti oggetti:

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

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

Le modalità di archiviazione sono regolamentate dal responsabile dell'RSP.

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

## **11. DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO**

### **11.1 Generalità**

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del servizio di protocollo, in base agli UU di appartenenza, ovvero in base alle rispettive competenze (UOP, 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), e una privata o riservata di autenticazione (password);

- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

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

## **11.2 Abilitazioni interne ad accedere ai servizi di protocollo**

Gli utenti abilitati accedono al PdP fornendo le credenziali di accesso che costituiscono le informazioni minime per controllare l'accesso al servizio e per identificare l'utente abilitato.

L'informazione relativa alla password è crittografata e accessibile soltanto da un processo di sistema.

# **12. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA**

## **12.1 Il registro di emergenza**

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

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

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

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

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

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

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

La funzionalità del PdP che realizza il registro di emergenza con un applicativo specifico, da installare sulle postazioni di lavoro della AOO in modalità stand alone, fuori linea, è in corso di realizzazione.

## **12.2 Modalità di apertura del registro di emergenza**

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica real time, le operazioni di protocollo siano svolte sul registro di emergenza informatico su postazioni di lavoro operanti fuori linea.

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

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

Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RSP predisporrà un apposito modulo.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile della tenuta del protocollo autorizza l'uso del registro di

emergenza per periodi successivi di durata non superiore ad una settimana.

### **12.3 Modalità di utilizzo del registro di emergenza**

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

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

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

### **12.4 Modalità di chiusura e di recupero del registro di emergenza**

E' compito del RSP verificare la chiusura del registro di emergenza.

E' compito del RSP, o di un suo delegato, riportare dal registro di emergenza al registro di protocollo generale del PdP le protocollazioni relative ai documenti protocollati in emergenza attraverso le postazioni di lavoro abilitate, entro cinque giorni dal ripristino delle funzionalità del PdP.

Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza, annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura. Per semplificare la procedura di chiusura del registro di emergenza il RSP utilizza il modulo utilizzato nella fase di apertura del registro di emergenza.

## **13. GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI**

### **13.1 Matrice delle correlazioni**

I procedimenti amministrativi sono descritti nell' "Elenco dei procedimenti amministrativi", di cui il RSP cura l'aggiornamento, estemporaneo o periodico.

I procedimenti amministrativi costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'amministrazione/ AOO.

All'interno dell'elenco i procedimenti sono individuati mediante la definizione dei riferimenti riportati al successivo paragrafo 13.2.

La definizione del singolo procedimento amministrativo rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.

Il risultato concreto di questa attività sono i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare.

L'individuazione del RPA e del responsabile dell'adozione del provvedimento finale è effettuata sulla base delle competenze assegnate a ciascuna figura interna alle UO/UU.

### **13.2 Elenco dei procedimenti amministrativi**

La gestione delle attività e dei procedimenti amministrativi, il loro iter, l'individuazione del responsabile del provvedimento finale e i termini entro i quali il procedimento deve essere concluso sono definiti così come previsto da norme di rango legislativo, regolamentari nonché dal regolamento interno emanato dall'amministrazione.

A tal fine l'AOO, per favorire la trasparenza dell'azione amministrativa, per semplificare i procedimenti e per schematizzare le descrizioni, costituisce una base informativa dei procedimenti amministrativi registrando, per ciascuno di essi, almeno, le seguenti informazioni:

- la denominazione e l'oggetto del procedimento;
- la normativa di riferimento;
- le fasi operative del procedimento (e, all'occorrenza, dei sub-procedimenti) e la relativa sequenza;
- il servizio competente;

- il responsabile del procedimento amministrativo;
- il responsabile dell'adozione del provvedimento finale;
- il tempo massimo di definizione dell'intero procedimento;
- eventuale operatività del silenzio assenso, del silenzio rifiuto o della segnalazione certificata di inizio attività;
- il nome del soggetto a cui è attribuito, in caso di inerzia, il potere sostitutivo, nonché le modalità per attivare tale potere, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale;
- soggetti esterni e/o altri servizi interni coinvolti;
- il titolare a cui il procedimento si riferisce, se disponibile.

### **13.3 Avvio dei procedimenti e gestione degli stati di avanzamento**

Mediante l'assegnazione dei fascicoli alle UO/UU di volta in volta competenti, le UOP o i RPA provvedono a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente.

La registrazione degli stati di avanzamento dei procedimenti amministrativi sulla base informativa sopra richiamata può avvenire in modalità manuale o automatica.

Nel primo caso, gli stati di avanzamento sono aggiornati dal RPA.

Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

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

### **14. Modalità di approvazione e aggiornamento del manuale**

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

Il presente manuale potrà essere aggiornato a seguito di:

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

#### **14.1 Regolamenti abrogati**

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

#### **14.3 Pubblicità del presente manuale**

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

Inoltre copia del presente manuale è:

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

#### **14.4 Operatività del presente manuale**

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



## 15. ALLEGATI

### 15.1 Definizioni

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

ARCHIVIAZIONE ELETTRONICA	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (Si veda l'art.1 della deliberazione CNIPA 19 febbraio 2004 n.11)
AREA ORGANIZZATIVA (AOO) OMOGENEA	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato (Si veda l'art.2, lettera n) del dPCM 31 ottobre 2000)
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o dell'affare, cui i documenti si riferiscono
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (l'art 1., comma 1, lettera i) del dPR 28 dicembre 2000, n. 445)
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; (art. 1, comma 1 lettera b) del d. lgs.7 marzo 2005, n.82)
BANCA DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art.4 comma 1 lettera p) del d. lgs 30 giugno 2003 n.196)
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (art.4, comma 1, lettera. o) del d. lgs 30 giugno 2003 n.196)
CARTA NAZIONALE DEI SERVIZI	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (art. 1 lettera d del d.lgs.7 marzo 2005, n.82)
CARTA D'IDENTITÀ ELETTRONICA	Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare (art. 1 comma 1 , lettera c) del d.lgs.7 marzo 2005, n.82)
CASELLA DI POSTA ELETTRONICA ISTITUZIONALE	La casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del D.P.C.M. 31 ottobre 2000, articolo 15, comma 3).(Si veda l'art. 1 dell'allegato A alla circolare AIPA 7 maggio 2001 n. 28)
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi. (Si veda l'art. 1, comma 1 lettera e) del d.lgs.7 marzo 2005, n.82
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I
CERTIFICATO	Il documento rilasciato da una Amministrazione Pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (art.1, comma 1 lettera f) del dPR 28

	dicembre 2000, n. 445)
CERTIFICATORE	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art. 1 , comma 1 lettera g) del d.lgs. 7 marzo 2005, n.82)
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art.4, comma 1, lettera l) del d. lgs 30 giugno 2003 n.196)
CONSERVAZIONE SOSTITUTIVA CREDENZIALI DI AUTENTICAZIONE	Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004; n.11. I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art.4 comma 3 lettera d) del d.lgs. 30 giugno 2003 n.196);
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del dPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art.4, comma 1 lettera e) del d.lgs. 30 giugno 2003 n.196)
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato (art.4, comma 1 lettera c) del d.lgs. 30 giugno 2003 n.196)
DATI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art.4, comma 1, lettera d) del d.lgs. 30 giugno 2003 n.196)
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art.4 comma 1 lettera n) del d.lgs 30 giugno 2003 n.196)
DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art.4 comma 1 lettera b) del d.lgs. 30 giugno 2003 n.196)
DATO PUBBLICO	Il dato conoscibile da chiunque (art. 1, comma 1, lettera n) del d.lgs..7 marzo 2005, n.82)
DATO A CONOSCIBILITÀ LIMITATA	Il dato la cui conoscibilità riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. 1, comma 1, lettera

	l) del d. lgs.7 marzo 2005, n.82)
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal art.1, comma 1, lettera h) del dPR 28 dicembre 2000, n. 445
DICHIARAZIONE DI CERTIFICAZIONE SOSTITUTIVA	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato (Si veda l'art.1, comma 1, lettera g) del dPR 28 dicembre 2000, n. 445)
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art.4, lettera m) del d.lgs. 30 giugno 2003 n.196)
DOCUMENTO	Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (art 1, comma 1, lettera a) della deliberazione CNIPA del 19 febbraio 2004 n. 11)
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa ( Si veda art. 1 comma 1, lettera a) del dPR 28 dicembre 2000, n. 445)
DOCUMENTO ANALOGICO	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (ad esempio: documenti cartacei), come le immagini su film (ad esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (ad esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art 1, comma 1, lettera b). della deliberazione CNIPA del 19 febbraio 2004, n.11)
DOCUMENTO ANALOGICO ORIGINALE	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art 1. della deliberazione CNIPA del 19 febbraio 2004, n.11)
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (Si veda art 1, comma 1, lettera h) della deliberazione CNIPA del 19 febbraio 2004 n.11)
DOCUMENTO CONSERVATO	Documento sottoposto al processo di conservazione sostitutiva (art 1. deliberazione CNIPA del 19 febbraio 2004, n.11)
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare (art. 1 comma 1, lettera c) del dPR 28 dicembre 2000, n. 445)
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del titolare (art.1, comma 1, lettera d) del dPR 28 dicembre 2000, n. 445)

DOCUMENTO D'IDENTITÀ ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (art.1, comma 1, lettera.e) del DPR 28 dicembre 2000, n.445 )
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lettera t) del d.lgs. 7 marzo 2005, n.82)
DOSSIER	Aggregazione di più fascicoli che può essere costituito a seguito di esigenze operative dell'Amministrazione, come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia (art.1, comma 1, lettera n) della deliberazione AIPA 19 febbraio 2004, n.11)
EVIDENZA INFORMATICA	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art.1, comma 1, lettera f) del dPCM 13 gennaio 2004)
FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi
FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento delle attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati da insiemi di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). I fascicoli costituiscono il tipo di unità archivistica più diffuso degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, comma 1, lettera s) del d.lgs.7 marzo 2005, n.82)
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lettera q) del d.lgs. 7 marzo 2005, n.82)
FIRMA ELETTRONICA QUALIFICATA	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e

	collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1, comma 1 , lettera r) del d.lgs.7 marzo 2005, n.82)
FORMAZIONE INFORMATICA DEI DOCUMENTI	Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa. (art.2 lettera c della deliberazione AIPA 23 novembre 2000 n. 51)
FUNZIONE DI HASH	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (art.1, comma 1, lettera e) del dPCM 13 gennaio 2004
GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del d.lgs. 30 giugno 2003 n.196, istituita dalla legge 31 dicembre 1996, n. 675 (Si veda art.4 comma 1 lettera g) del d.lgs. 30 giugno 2003 n.196)
GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1 comma 1 lett m del d.lgs. 7 marzo 2005, n. 82)
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art.1 del dPCM 13 gennaio 2004)
INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
INSERTO	Sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa. (art.1 comma 1 lett. 1) del DPR 28 dicembre 2000, n. 445)
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica Amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato.(art.1, comma 1, lettera n) del DPR 28 dicembre 2000, n. 445)
MARCA TEMPORALE	Evidenza informatica che consente la validazione temporale (art.1, comma 1, lettera m) del dPCM 13 gennaio 2004)
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	Strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni, e

	<p>sottopartizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti.</p> <p>Indica per ciascun procedimento/procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello Stato o per la sezione degli archivi storici per gli Enti pubblici) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il piano di conservazione periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali</p>
MEMORIZZAZIONE	<p>Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'art. 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del d.lgs. 23 gennaio 2002, n. 10 (art 1, comma 1, lettera f) della deliberazione CNIPA del 19 febbraio 2004 n.11)</p>
MISURE MINIME DI SICUREZZA	<p>Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 del d.lgs 30 giugno 2003 n.196. (Si veda art.4 comma 3 lettera a) del d.lgs. 30 giugno 2003 n.196)</p>
PAROLA CHIAVE	<p>Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o di altri dati in forma elettronica (art.4, comma 3, lettera e) del d.lgs. 30 giugno 2003, n.196)</p>
ORIGINALI NON UNICI	<p>I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art 1, comma 1, lettera v) del d.lgs..7 marzo 2005, n.82)</p>
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	<p>Vedi massimario di selezione e scarto</p>
PROFILO DI AUTORIZZAZIONE	<p>L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (art.4, comma 3, lettera f) del d.lgs. 30 giugno 2003 n.196)</p>
PUBBLICO UFFICIALE	<p>Il notaio, salvo quanto previsto dall'art. 5, comma 4 della deliberazione CNIPA del 19 febbraio 2004, n.11 e casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Si veda art 1 lettera q. della deliberazione CNIPA del 19 febbraio 2004, n.11)</p>
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI	<p>La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art.4, comma 1, lettera g) del d.lgs. 30 giugno 2003 n.196)</p>

RESPONSABILE DELSERVIZIO DI PROTOCOLLO	Il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'articolo 62, comma 2, del dPR 28 dicembre 2000, n. 445
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI (RPA) RIFERIMENTO TEMPORALE	Persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art 1,, comma 1, lettera g) del dPCM 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (Si veda art. 1, comma 1, lettera i), del dPR 11 febbraio 2005, n.68
RIVERSAMENTO DIRETTO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (art , comma 1 , lettera n) . della deliberazione CNIPA del 19 febbraio 2004, n. 11).
RIVERSAMENTO SOSTITUTIVO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (art 1, comma 1, lettera o) della deliberazione CNIPA del 19 febbraio 2004, n. 11 )
SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (art.4, comma 4, lettera c) del d.lgs. 30 giugno 2003 n.196)
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (art.4, comma 4, lettera b) del d.lgs. 30 giugno 2003 n.196)
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (art.4, comma 4, lettera a) del d.lgs. 30 giugno 2003 n.196)
SEGNATURA INFORMATICA	L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'articolo 18, comma 1, del dPCM 31 ottobre 2000 (art.1 dell'allegato A circolare AIPA 7 maggio 2001 n.28)
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso (Glossario dell'IPA Indice delle Pubbliche Amministrazioni)
SISTEMA DI CLASSIFICAZIONE	Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (art.2, comma 1, lettera h) del dPCM 31ottobre 2000)
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art.4, comma 3, lettera g) del d.lgs. 30 giugno 2003 n.196)
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1, comma 1, lettera r) del dPR 28 dicembre 2000 n.445)
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico, o comunque automatizzato con cui si

## 15.2 Area organizzativa omogenea e modello organizzativo

### Modello Organizzativo dell'Amministrazione

Denominazione dell'Amministrazione	Comune di Policoro
Codice Identificativo assegnato dell'Amministrazione	G786
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Piazza Aldo Moro, 1 75025 – Policoro (MT)
AREA ORGANIZZATIVA OMOGENEA - AOO	Comune di Policoro

### La struttura organizzativa prevede una sola Area Organizzativa Omogenea

Denominazione dell'Area Organizzativa Omogenea	<b>Comune di Policoro</b>
Codice Identificativo assegnato alla AOO	<b>1</b>
Responsabile del servizio di protocollo informatico, gestione documentale e archivistica	<b>Individuato con decreto sindacale</b>
Casella di posta elettronica istituzionale dell'AOO	<b>protocollo@pec.policoro.gov.it</b>
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale	<b>Piazza Aldo Moro, 1 75025 – Policoro (MT)</b>

### Articolazione dell'AOO in Unità Organizzative:

Settore	U.O. Ufficio	Tipo protocollo
	Ufficio Staff Sindaco	Registrazione Uscita
	Ufficio Staff Polizia Locale	Registrazione in Ingresso/Uscita
<b>I Settore</b>	Organi istituzionali - Segreteria	Registrazione Uscita
	Gare e Contratti	Registrazione Uscita
	Registrazione di Protocollo – UOP	Registrazione in Ingresso/Uscita
	Ufficio Stato civile / Anagrafe-/ Elettorale	Registrazione Uscita
	Servizi alle persone	Registrazione Uscita
	Pubblica Istruzione attività culturali- Biblioteca	Registrazione in Ingresso/Uscita
	Ufficio turismo- sport- spettacolo	Registrazione Uscita
<b>II Settore</b>	Ufficio personale – ragioneria	Registrazione Uscita
	Servizio tributi	Registrazione Uscita
	Servizio economato	Registrazione Uscita
<b>III Settore</b>	Segreteria tecnica	Registrazione Uscita
	Sportello Unico Edilizia	Registrazione in Ingresso/Uscita
	Servizi al territorio	Registrazione Uscita

	Urbanistica/Edilizia privata	
	Lavori Pubblici	Registrazione Uscita
	Servizio Patrimonio	Registrazione Uscita
<b>IV Settore</b>	SUAP- Polizia Amministrativa- Protezione Civile	Registrazione Uscita

L'organigramma completo e aggiornato è presente in Internet sul sito [www.policoro.gov.it](http://www.policoro.gov.it).

## 15.3 Politiche di sicurezza

### Classificazione della sicurezza

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

- Pubblico. Si riferisce a componenti o informazioni che non richiedono protezione specifica;
- Interno. E' richiesto per componenti o informazioni con divieto di divulgazione all'esterno della AOO oppure di proprietà o di consultazione di terze parti autorizzate. Sono classificati a questo livello:
  - ✓ i dati personali comuni, salvo particolari esigenze;
  - ✓ i registri di protocollo se non contenenti dati personali sensibili e giudiziari.
- Confidenziali: è assegnato ai componenti o informazioni rilevanti ai fini della sicurezza o per la conduzione del Centro Elaborazione Dati oppure di proprietà o di consultazione di terze parti autorizzate con le quali è stabilito un formale accordo scritto. Sono considerati materiali confidenziali e classificati a questo livello:
  - ✓ i dati personali sensibili e giudiziari, salvo esigenze più restrittive;
  - ✓ i registri di protocollo contenenti dati personali sensibili e giudiziari;
  - ✓ documenti e supporti rimovibili contenenti dati appartenenti alle Amministrazioni (servizio Gestione Documentale);
  - ✓ documenti critici ai fini della sicurezza (specifiche di progettazione, configurazione, di indirizzamento, ecc.);
  - ✓ log di sicurezza;
  - ✓ risultati dei test di penetrabilità e degli audit;
  - ✓ report dei livelli di servizio;
  - ✓ gli archivi che il Servizio Informatico è impegnato a conservare per disposizioni di legge.
- Altamente riservato. E' richiesto per componenti o informazioni di particolare rilevanza la cui diffusione può arrecare un pericolo immediato dal punto di vista della sicurezza o un danno notevole per la conduzione del Centro. Le password e le eventuali chiavi di crittografia sono classificate a questo livello.

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

### Utilizzo del servizio di protocollo

#### Configurazione della postazione di lavoro - BROWSER

L'utilizzo dell'applicativo software per il protocollo informatico avviene in modalità client server con le postazioni configurate con l'apposito programma e il browser previsto per l'eventuale utilizzo di servizi web di protocollo sarà Internet Explorer da ver. 8.0 in poi, Mozilla Firefox e Google Chrome.

## **Configurazione della postazione di lavoro - ANTIVIRUS**

I posti di lavoro devono essere dotati di un prodotto antivirus installato a cura e spese dell'Amministrazione/AOO al fine di prevenire la diffusione di software malevolo (virus e worms) proteggendo sia la stazione di lavoro che le reti alle quali l'utente è collegato.

E' responsabilità dell'utente verificarne la presenza, l'attivazione del monitor real-time e l'aggiornamento delle virus signatures. È necessario configurare una modalità di aggiornamento automatica con periodicità giornaliera.

## **Gestione dell'utenza**

La responsabilità delle azioni compiute nella fruizione del servizio di protocollo è dell'utente fruitore del servizio.

Gli utenti autorizzati ad accedere al servizio di protocollo dispongono di una propria credenziale personale, costituita da una parte pubblica ed una riservata.

Ogni nuovo utente autorizzato viene registrato secondo una specifica procedura con la quale vengono annotate le informazioni relative all'utente, alla sua credenziale pubblica, la qualifica e i diritti d'accesso.

La coppia di credenziali non deve mai essere ceduta a terzi. La responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo titolare, anche se compiute in sua assenza.

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

- La stazione di lavoro non deve essere lasciata incustodita, anche per brevi periodi, con la sessione attiva, prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla stazione di lavoro (ad esempio, blocco tramite Ctrl-Alt-Canc con password locale).
- In generale deve essere adottata la politica della cosiddetta "scrivania pulita" che obbliga a non lasciare materiale riservato incustodito al di fuori dell'orario di lavoro e invita a riporre il materiale di lavoro (documenti, supporti) negli appositi armadi, secondo il livello di sicurezza, di disattivare la stazione di lavoro, di tenere chiusi i locali.

## **Segnalazioni di malfunzionamento o problemi di sicurezza**

E' compito di tutto il personale utente vigilare sull'osservanza delle misure di sicurezza, di segnalare possibili problemi relativi alla sicurezza o all'erogazione del servizio, di porre in atto le misure ed i comportamenti previsti dalle norme al fine di raggiungere e mantenere il livello di sicurezza e di servizio prefissato, in rapporto alle proprie mansioni e capacità.

Le segnalazioni relative a carenze di sicurezza o a malfunzionamenti che possono generare problemi di sicurezza possono essere indirizzate direttamente al CED o al servizio di sicurezza.

## **15.4 Regole di gestione della corrispondenza convenzionale in ingresso e in uscita al/dal servizio postale**

La corrispondenza in ingresso è consegnata direttamente all'UOP.

La corrispondenza è quotidianamente consegnata al/dal personale dell'UOP dell'AOO, al servizio postale.

La corrispondenza in uscita, raccolta e predisposta dall'UOP medesima, è consegnata quotidianamente in busta chiusa al suddetto servizio postale.

Gli Uffici Utente devono far pervenire la posta in partenza all'UOP che esegue la spedizione, entro le ore 12.30 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP, che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

## **15.5 Elenco dei documenti esclusi dalla registrazione di protocollo**

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

- Gazzette ufficiali, Bollettini ufficiali PA;
- Notiziari PA;
- Giornali, Riviste, Libri;
- Materiali pubblicitari;
- Note di ricezione circolari;
- Note di ricezione altre disposizioni;
- Materiali statistici;
- Atti preparatori interni;
- Offerte o preventivi di terzi non richiesti;
- Inviti a manifestazioni che non attivino procedimenti amministrativi;
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.);
- Allegati, se accompagnati da lettera di trasmissione, ivi compresi gli elaborati tecnici;
- Certificati e affini;
- Determinazioni;
- Le ricevute di ritorno delle raccomandate A.R.;
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico- amministrativa presente o futura;
- Corsi di aggiornamento;
- Pubblicità conoscitiva di convegni;
- Pubblicità in generale;
- Offerte e Listini prezzi;
- Deliberazioni del Consiglio comunale;
- Deliberazioni della Giunta comunale;
- Non saranno registrate a protocollo le certificazioni anagrafiche rilasciate direttamente al richiedente, le richieste e/o trasmissioni di certificati e tutta la corrispondenza dell'anagrafe, stato civile e leva diretta agli uffici comunali;

## **15.6 Elenco dei documenti soggetti a registrazione particolare**

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto, all'interno dell'AOO, un protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati. In questo ambito rientrano:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- i documenti anonimi, individuati ai sensi dell'art. 8, commi 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241 e dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge n. 196/2003 (e successive modifiche ed integrazioni) e norme collegate.

## 15.7 Titolario di classificazione

### Titolo I. Amministrazione generale

1. Legislazione e circolari esplicative
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
3. Statuto
4. Regolamenti
5. Stemma, gonfalone, sigillo
6. Archivio generale
7. Sistema informativo
8. Informazioni e relazioni con il pubblico
9. Politica del personale; ordinamento degli uffici e dei servizi
10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale
11. Controlli interni ed esterni
12. Editoria e attività informativo-promozionale interna ed esterna
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
14. Interventi di carattere politico e umanitario; rapporti istituzionali
15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni
16. Area e città metropolitana
17. Associazionismo e partecipazione

### Repertori

- Registro di protocollo
- Registro dell'Albo pretorio
- Registro delle notifiche
- Ordinanze emanate dal Sindaco: serie con repertorio
- Decreti del Sindaco: serie con repertorio
- Ordinanze emanate dai dirigenti
- Determinazioni dei dirigenti
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Verbali delle adunanze del Consiglio comunale
- Verbali delle adunanze della Giunta comunale
- Verbali degli organi collegiali del Comune
- Contratti e convenzioni
- Albo dell'associazionismo: elenco delle associazioni accreditate
- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)

## **Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia**

1. Sindaco
2. Vice-sindaco
3. Consiglio
4. Presidente del Consiglio
5. Conferenza dei capigruppo e Commissioni del Consiglio
6. Gruppi consiliari
7. Giunta
8. Commissario prefettizio e straordinario
9. Segretario e Vice-segretario
10. Direttore generale e dirigenza
11. Revisori dei conti
12. Difensore civico
13. Commissario ad acta
14. Organi di controllo interni
15. Organi consultivi

### **Titolo III. Risorse umane**

1. Concorsi, selezioni, colloqui
2. Assunzioni e cessazioni
3. Comandi e distacchi; mobilità
4. Attribuzione di funzioni, ordini di servizio e missioni
5. Inquadramenti e applicazione contratti collettivi di lavoro
6. Retribuzioni e compensi
7. Trattamento fiscale, contributivo e assicurativo
8. Tutela della salute e sicurezza sul luogo di lavoro
9. Dichiarazioni di infermità ed equo indennizzo
10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza
11. Servizi al personale su richiesta
12. Orario di lavoro, presenze e assenze
13. Giudizi, responsabilità e provvedimenti disciplinari
14. Formazione e aggiornamento professionale
15. Collaboratori esterni

#### **Serie**

Fascicoli del personale: un fascicolo per ogni dipendente o assimilato

#### **Repertori**

- Registro infortuni
- Elenco degli incarichi conferiti
- Verbali dei rappresentanti dei lavoratori per la sicurezza

#### **Titolo IV. Risorse finanziarie e patrimoniali**

1. Bilancio preventivo e Piano esecutivo di gestione (PEG)
2. Gestione del bilancio e del PEG (con eventuali variazioni)
3. Gestione delle entrate: accertamento, riscossione, versamento
4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
5. Partecipazioni finanziarie
6. Rendiconto della gestione; adempimenti e verifiche contabili
7. Adempimenti fiscali, contributivi e assicurativi
8. Beni immobili
9. Beni mobili
10. Economato
11. Oggetti smarriti e recuperati
12. Tesoreria
13. Concessionari ed altri incaricati della riscossione delle entrate
14. Pubblicità e pubbliche affissioni

#### **Repertori**

Mandati Reversali

Concessioni di occupazione suolo pubblico Concessioni di beni del demanio statale erregionale

## **Titolo V. Affari legali**

1. Contenzioso
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni
3. Pareri e consulenze

## **Titolo VI. Pianificazione e gestione del territorio**

1. Urbanistica: Regolamento Urbanistico, Piano Strutturale e varianti
2. Urbanistica: strumenti di attuazione dei Piani urbanistici generali.
3. Edilizia privata
4. Edilizia pubblica
5. Opere pubbliche
6. Catasto
7. Viabilità
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
9. Ambiente: autorizzazioni, monitoraggio e controllo
10. Protezione civile ed emergenze

### **Repertori**

- Concessioni edilizie
- Autorizzazioni paesaggistiche
- Certificati di agibilità

## **Titolo VII. Servizi alla persona**

1. Diritto allo studio e servizi
2. Asili nido e scuola materna
3. Promozione e sostegno delle istituzioni di istruzione e della loro attività
4. Orientamento professionale; educazione degli adulti; mediazione culturale
5. Istituti culturali (Musei, biblioteche, teatri , etc.)
6. Attività ed eventi culturali
7. Attività ed eventi sportivi
8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio
10. Informazione, consulenza ed educazione civica
11. Tutela e curatela di incapaci
12. Assistenza diretta e indiretta, benefici economici
13. Attività ricreativa e di socializzazione
14. Politiche per la casa
15. Politiche per il sociale

### **Repertori**

- Verbali degli organi di gestione degli Istituti culturali

## **Titolo VIII. Attività economiche**

1. Agricoltura e pesca
2. Artigianato
3. Industria
4. Commercio
5. Fiere e mercati
6. Esercizi turistici e strutture ricettive
7. Promozione e servizi

### **Serie**

Fascicoli individuali di ciascun esercente attività economiche

## **Titolo IX. Polizia locale e sicurezza pubblica**

1. Prevenzione ed educazione stradale
2. Polizia stradale
3. Informative
4. Sicurezza e ordine pubblico

### **Repertori**

- Autorizzazioni di pubblica sicurezza
- Verbali degli accertamenti

## **Titolo X. Tutela della salute**

1. Salute e igiene pubblica
2. Trattamenti Sanitari Obbligatori
3. Farmacie
4. Zooprofilassi veterinaria
5. Randagismo animale e ricoveri

### **Repertori**

- Repertorio delle autorizzazioni sanitarie

## **Titolo XI. Servizi demografici**

1. Stato civile
2. Anagrafe e certificazioni
3. Censimenti
4. Polizia mortuaria e cimiteri

### **Repertori**

- Registro dei nati
- Registro dei morti
- Registro dei matrimoni
- Registro di cittadinanza
- Registro della popolazione
- Registri di seppellimento
- Registri di tumulazione
- Registri di esumazione
- Registri di estumulazione
- Registri di cremazione
- Registri della distribuzione topografica delle tombe con annesse schede onomastiche

## **Titolo XII. Elezioni e iniziative popolari**

1. Albi elettorali
2. Liste elettorali
3. Elezioni
4. Referendum
5. Istanze, petizioni e iniziative popolari

### **Repertori**

- Verbali della commissione elettorale comunale
- Verbali dei presidenti di seggio

### **Titolo XIII. Affari militari**

1. Leva e servizio civile sostitutivo
2. Ruoli matricolari
3. Caserme, alloggi e servitù militari
4. Requisizioni per utilità militari

## **Titolo XIV. Oggetti diversi**