Consiglio regionale della Puglia

Sezione Informatica e Tecnica

MANUALE DI GESTIONE DOCUMENTALE DEL CONSIGLIO REGIONALE DELLA PUGLIA

Aggiornato al 22 febbraio 2016

Redazione a cura di:

Dott.ssa Anna Giulia CALVANI (P.O. "Protocollo informatico-archivio-posta - Responsabile Gestione Documentale)
Dott. Vito Fiore PISCOPO (A.P. Sistemi Informatici e Tecnici -Vicario Responsabile Gestione Documentale)

Coordinamento: Sezione Informatica e Tecnica:

Dott. Dott. Riccardo SANNA (Dirigente della Sezione)

Supporto tecnico-scientifico:

Ing. Carmelo TOMMASI (Direttore Tecnico società Cadan S.r.l. – Bari)

INDICE

TITOLO I DISPOSIZIONI GENERALI 5

ARTICOLO 1 - PREMESSA 5
ARTICOLO 2 - AMBITO DI APPLICAZIONE DEL MANUALE 6
ARTICOLO 3 - DEFINIZIONI E NORME DI RIFERIMENTO 7

TITOLO II STRUTTURA ED ORGANIZZAZIONE 9

ARTICOLO 4 - AREA ORGANIZZATIVA OMOGENEA E MODELLI ORGANIZZATIVI 9
ARTICOLO 5 - SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO 9
ARTICOLO 6 - RESPONSABILE DELLA GESTIONE DOCUMENTALE 10
ARTICOLO 7 - ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA 10
ARTICOLO 8 - CASELLE DI POSTA ELETTRONICA 11
ARTICOLO 9 - SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI 11
ARTICOLO 10 - FORMAZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO 11
ARTICOLO 11 - FIRMA DIGITALE 12
ARTICOLO 12 - TUTELA DEI DATI PERSONALI 12
ARTICOLO 13 - FORMAZIONE 13
ARTICOLO 14 - SORGENTE INTERNA DEI DOCUMENTI 14
ARTICOLO 15 - VERIFICA FORMALE DEI DOCUMENTI 14
ARTICOLO 16 - TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA 14
Articolo 16.1 Affrancatura dei documenti in partenza 15
Articolo 16.2 Conteggi spedizione corrispondenza 15
Articolo 16.3 Documenti in partenza per posta convenzionale con più destinatari. 16
ARTICOLO 17 - TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO FAX 16
Articolo 17.1 Inserimento delle ricevute di trasmissione nel fascicolo 16
ARTICOLO 18 - ORARI DI ACCESSO ALLA STRUTTURA DI PROTOCOLLO E SPEDIZIONE POSTA 16

TITOLO III ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO 17

ARTICOLO 19 - PIANO DI ATTUAZIONE 17

TITOLO IV PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI 18

ARTICOLO 20 - DEFINIZIONE 18
ARTICOLO 21 - OBIETTIVI DEL PIANO DI SICUREZZA 18
ARTICOLO 22 - REDAZIONE E REVISIONI 18
ARTICOLO 23 - MISURE DI SICUREZZA PER LA FORMAZIONE DEI DOCUMENTI INFORMATICI 19
ARTICOLO 24 - MISURE DI SICUREZZA PER LA GESTIONE DEI DOCUMENTI INFORMATICI 19
Articolo 24.1 Componente organizzativa della sicurezza 20
Articolo 24.2 Componente fisica della sicurezza 21
Articolo 24.3 Componente logica della sicurezza 21
Articolo 24.4 Componente infrastrutturale della sicurezza 21
Articolo 24.5 Gestione delle registrazioni di sicurezza 22
ARTICOLO 25 - MISURE DI SICUREZZA PER LA TRASMISSIONE E L'INTERSCAMBIO DEI DOCUMENTI INFORMATICI 22
Articolo 25.1 Interscambio con altre AOO 23
Articolo 25.2 Interscambio all'interno della AOO 23
ARTICOLO 26 - ACCESSO AI DOCUMENTI INFORMATICI 23
Articolo 26.1 Utenti interni alla AOO 24
Articolo 26.2 Accesso al registro di protocollo per utenti interni alla AOO 25
Articolo 26.3 Utenti esterni alla AOO - Altre AOO/Amministrazioni 25
Articolo 26.4 Utenti esterni alla AOO - Privati 25
ARTICOLO 27 - CONSERVAZIONE DEI DOCUMENTI INFORMATICI 26

GESTIONE DEI FLUSSI DOCUMENTALI 27

ARTICOLO 28 - FLUSSI DOCUMENTALI IN INGRESSO 27
Articolo 28.1 Ricezione 27

Articolo 28.2 Protocollazione *28*
Articolo 28.3 Segnatura di protocollo dei documenti *29*
Articolo 28.4 Assegnazione *29*
ARTICOLO 29 - FLUSSI DOCUMENTALI IN USCITA 29
Articolo 29.1 Formazione del documento *29*
Articolo 29.2 Sottoscrizione *30*
Articolo 29.3 Registrazione di protocollo *30*
Articolo 29.4 Spedizione *30*
Articolo 29.5 Utilizzo del fax tra pubbliche amministrazioni *30*
ARTICOLO 30 - FLUSSI DOCUMENTALI INTERNI ALL'AOO 30
ARTICOLO 31 - DOCUMENTI DA NON SOTTOPORRE A REGISTRAZIONE OBBLIGATORIA NEL PROTOCOLLO GENERALE 31
ARTICOLO 32 - REGISTRO GIORNALIERO DI PROTOCOLLO 31
ARTICOLO 33 - ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO 31
ARTICOLO 34 - GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL SDP 32
ARTICOLO 35 - IL REGISTRO DI EMERGENZA 32

TITOLO V CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIAZIONE DEI DOCUMENTI 34

ARTICOLO 36 - TITOLARIO DI CLASSIFICAZIONE 34
Articolo 36.1 Attribuzione del codice di classificazione ai documenti *34*
ARTICOLO 37 - FASCICOLAZIONE DEI DOCUMENTI 34
ARTICOLO 38 - ARCHIVIAZIONE DEI DOCUMENTI 35
Articolo 38.1 Archiviazione dei documenti elettronici *36*
Articolo 38.2 Archiviazione dei documenti cartacei *36*
Articolo 38.3 7.3.3. Piano di conservazione dell'archivio *36*
Articolo 38.4 Versamento dei fascicoli nell'archivio di deposito *36*
Articolo 38.5 Sistema di conservazione dei documenti informatici *37*

TITOLO VI ALLEGATI AL MANUALE DI GESTIONE DEL DOCUMENTALE DEL CONSIGLIO REGIONALE DELLA PUGLIA 38

TITOLO I DISPOSIZIONI GENERALI

Articolo 1 - Premessa

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le nuove "Regole tecniche per il protocollo informatico *ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005* - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario, prevede, per tutte le amministrazioni di cui all'art. 2, comma 2 del decreto legislativo 7 marzo 2005, n. 82, l'adozione del *Manuale di gestione* (**MdG**) adeguato alle nuove regole tecniche. Quest'ultimo infatti, è specificatamente disciplinato dall'art. 5 del citato DPCM 3 dicembre 2013.

Obiettivo del Manuale di Gestione aggiornato è di descrivere il sistema di gestione, anche ai fini della conservazione a norma, dei documenti informatici e di fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, a partire dalla fase di protocollazione della corrispondenza in ingresso, in uscita e interna, nonché delle funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'Amministrazione.

In tale ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un Responsabile per la *gestione documentale* ed un suo Vicario, per i casi di vacanza, assenza o impedimento del primo.

Il presente documento pertanto si rivolge non solo agli operatori di protocollo e agli istruttori delle pratiche, in quanto strumento di lavoro e di riferimento per la gestione dei documenti, degli affari e dei procedimenti amministrativi, ma, in generale, a tutti i dipendenti (dirigenti, funzionari, etc.) che a diverso titolo accedano ai documenti gestiti dall'Amministrazione ed ai soggetti esterni che si relazionino con la stessa.

Pertanto, saranno regolamentati:

- la pianificazione, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal testo unico;
- il piano di sicurezza relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso e alla conservazione dei documenti informatici;
- le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e di scambio degli stessi all'interno ed all'esterno dell'Area Organizzativa Omogenea, ivi comprese le caselle di posta elettronica e certificata utilizzate;
- la descrizione di eventuali ulteriori formati utilizzati per la formazione del documento informatico in relazione a specifici contesti operativi esplicitati e motivati;
- l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi;
- la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione;

- l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
- la migrazione dei flussi cartacei verso quelli digitali, ovvero come fase transitoria, i flussi cartacei in rapporto al protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo di processi e azioni amministrative;
- l'uso del titolario di classificazione e del massimario di selezione e scarto;
- le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche;
- le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, con indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire la *staticità, l'immodificabilità*, *l'integrità* e *la leggibilità* del registro giornaliero di protocollo;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse in attuazione della trasparenza dell'azione amministrativa.

Pertanto il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Tutto il personale del Consiglio è tenuto ad applicare le regole ivi contenute sotto il controllo e la supervisione del *Dirigente della Sezione Informatica e Tecnica.*

Poiché il manuale si compone di **disposizioni** di carattere generale, che presumibilmente rimarranno invariate nel tempo essendo le stesse legate alla disciplina normativa di Settore e di **specificazioni** di natura operativa o di dettaglio, che invece richiederanno un continuo adeguamento al contesto organizzativo, normativo e tecnologico del Consiglio, queste ultime sono riportate come allegati e costantemente aggiornate a cura del *Responsabile della gestione documentale* e, comunque, sotto il controllo e la supervisione del Dirigente della Sezione Informatica e Tecnica.

Il Manuale di Gestione del Protocollo Informatico del Consiglio regionale della Puglia è pubblicato sul Portale Ufficiale http://www.consiglio.puglia.it, come tra l'altro disposto dal comma 3, dell'art. 5, del citato DPCM 3 dicembre 2013.

Articolo 2 - Ambito di applicazione del manuale

Il presente Manuale di Gestione è adottato ai sensi dell'art. 3, comma d) del DPCM 3 dicembre 2013, recante le *regole tecniche per il protocollo informatico.*

In esso sono descritte le attività di sistema di gestione, anche ai fini della conservazione, dei documenti informatici e sono indicate le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali (quali formazione, registrazione, classificazione, fascicolazione) e dei flussi archivistici, in relazione ai

procedimenti amministrativi del Consiglio regionale della Puglia a partire dal 12 ottobre 2015, data di entrata in vigore delle nuove regole tecniche ai sensi del DPCM 3 dicembre 2013.

Attraverso la possibile integrazione con le procedure di gestione dei provvedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per il miglioramento del flusso informativo e documentale informatico interno dell'amministrazione anche ai fini dello snellimento e trasparenza dell'azione amministrativa.

Il protocollo conferisce certezza, anche sotto il profilo giuridico, dell'effettivo ricevimento e spedizione di un documento. È opportuna, al riguardo, in termini di efficienza, una visione integrata e moderna della gestione documentale, nell'arco del suo ciclo di vita, all'interno del sistema archivistico in cui la registrazione del protocollo è solo la fase iniziale.

La gestione integrata dei documenti, dei flussi documentali e dei procedimenti amministrativi, con modalità conformi al D.P.R. 28 dicembre 2000, n. 445, recante il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, e al nuovo codice dell'amministrazione digitale, contenuto nel D.lgs. 30 dicembre 2010, n. 235, e successive modificazioni e integrazioni, richiede non soltanto l'impiego di tecnologie avanzate, ma anche la revisione delle procedure inerenti alla tenuta del protocollo, dei documenti informatici e alla formazione dell'archivio.

Si è comunque consapevoli che la "semplice" attivazione di un sistema informatico di gestione documentale pur producendo effetti positivi sull'operatività dell'Ente per ottenere il massimo risultato deve essere anche accompagnato dalla reingegnerizzazione dei processi amministrativi e dalla rimodulazione delle attività di registrazione, classificazione, consultazione e archiviazione degli atti.

Articolo 3 - Definizioni e norme di riferimento

Ai fini del presente Manuale si intende per

Amministrazione	⇨	Il Consiglio regionale della Puglia
Archivio	⇨	Il complesso di documenti ricevuti o prodotti dall'Amministrazione nell'esercizio delle sue funzioni
Testo Unico	⇨	Il DPR del 20 dicembre 2000, n. 445 - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*
Regole tecniche	⇨	Il DPCM 3 dicembre 2013, *Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005* - Pubblicato in Gazzetta Ufficiale n. 59 del 12 marzo 2014 - supplemento ordinario
Regole tecniche per la Conservazione	⇨	Il DPCM 3 dicembre 2013, *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

Istruzioni Registro	⇨	le istruzioni emanate dall'Agenzia per l'Italia Digitale il 06/10/2015 per la *Produzione e Conservazione del registro giornaliero di protocollo*
Codice della Privacy	⇨	il D.lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali e successive modificazioni e integrazioni
Nuovo CAD	⇨	Il D.lgs. 30 dicembre 2010, n. 235 (*Nuovo Codice dell'amministrazione digitale*) - *Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale*.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

AOO	⇨	Area Organizzativa Omogenea, struttura individuate dall'Amministrazione, che opera su tematiche omogenee e presenta l'esigenza di gestire la documentazione in modo unitario e coordinato
MdG	⇨	Manuale di Gestione, come previsto all'art. 5 del DPCM 3 dicembre 2013
RPA	⇨	Responsabile Procedimento Amministrativo - il personale che ha la responsabilità dell'esecuzione degli adempimenti amministrativi e/o degli affari
RGD	⇨	Responsabile della Gestione Documentale, come previsto all'art. 4 del DPCM 3 dicembre 2013
VIC	⇨	Vicario del responsabile della Gestione Documentale, come previsto all'art. 3 del DPCM 3 dicembre 2013
DSIT	⇨	Dirigente della Sezione Informatica e Tecnica
SdP	⇨	Software di Protocollo informatico – l'applicativo DiDoc® acquisito dall'Amministrazione/AOO per implementare il servizio di protocollo informatico e la gestione documentale.
UOPG	⇨	Unità Organizzativa di registrazione Protocollo Generale - rappresenta la UO *Protocollo Informatico, Archivio, Posta, Telegrammi, Sms Istituzionali*
UOP	⇨	Unità Operative di registrazione di Protocollo - rappresentano le strutture distaccate dei Servizi del Consiglio e abilitati alla protocollazione, scansione e archiviazione dei documenti (IN PARTENZA, IN ARRIVO, INTERNO) dal proprio ambito.
UOR	⇨	Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato
PdV	⇨	Pacchetto di Versamento, ovvero un pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
AD	⇨	Atto Dirigenziale

Per tutte le altre definizioni è necessario fare riferimento all'Allegato 1 - *Glossario/Definizioni* - delle Regole Tecniche, da cui le presenti sono, in parte, state tratte.

TITOLO II STRUTTURA ED ORGANIZZAZIONE

Articolo 4 - Area Organizzativa Omogenea e modelli organizzativi

Per la gestione dei flussi documentali, informatici e analogici, del protocollo e dell'archivio, l'Amministrazione individua un'unica Area Organizzativa Omogenea (AOO), i cui dati identificativi sono riportati nell'***Allegato 1***. Mentre nell'***Allegato 2*** sono descritte le unità operative decentrate di registrazione protocollo.

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

Nell'unica AOO è istituita una struttura per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'interno dell'AOO tutta la documentazione con direzione "IN ARRIVO" dall'esterno, "*IN USCITA*" e "*INTERNO*" viene gestita con il sistema di protocollazione in forma decentralizzata per le UOR che svolgono anche i compiti di UOP, come indicato nell'***Allegato 2***. Al riguardo si è provveduto ad istruire ed a mantenere aggiornato il personale delle UOP e si è provveduto ad acquisire le relative autorizzazioni ed a dotare gli operatori di specifiche dotazioni HW e SW.

L'***Allegato 2*** è suscettibile di modifica in caso di definizione di nuove UOP o di riorganizzazione delle medesime.

Le modifiche sono proposte dal RGD alla funzione di governo dell'Amministrazione d'intesa con il Responsabile del Sistema Informativo, con il Responsabile della tutela dei dati personali e con la funzione di governo dell'Amministrazione.

L'Amministrazione si riserva la facoltà di autorizzare, per particolari esigenze, altri UOR allo svolgimento dell'attività di protocollazione.

Tale "decentramento" da un punto di vista operativo segue le norme stabilite nel presente Manuale e sarà sottoposto al controllo del RGD e sotto la supervisione del DSIT.

Negli UOR di cui sopra sarà utilizzata la medesima numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RGD che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

Articolo 5 - Servizio per la gestione informatica del protocollo

Nell'ambito dell'AOO di cui al TITOLO II è istituita una Unità Organizzativa (UOPG) per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, denominata *Protocollo Informatico, Archivio, Posta, Telegrammi, Sms Istituzionali*. A detta UOPG sono assegnati i compiti per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, il cui dettaglio è riportato in ***Allegato 14***. Detto allegato è suscettibile di modifica in caso di variazioni normative e/o organizzative del Consiglio regionale della Puglia deliberate dagli Organi competenti e/o dalla funzione di governo dell'Amministrazione.

Alla responsabilità della citata UOPG è posto il Responsabile della Gestione Documentale (RGD), alle dirette dipendenze del *Sezione Informatica e Tecnica* del Consiglio regionale della

Puglia, formalizzato con AD del DSIT di cui all'***Allegato 12***.

Articolo 6 - Responsabile della Gestione Documentale

Nell'ambito dell'AOO di cui al TITOLO II, in attuazione dell'art. 61 del Testo Unico «*al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente*» e dell'art. 3, comma 1, lettera b), sono nominati il **Responsabile della Gestione Documentale** ed il suo **Vicario**, per i casi di vacanza, assenza o impedimento del primo, con Atto Dirigenziale del DSIT.

In ***Allegato 12*** si riporta l'atto di nomina.

Al RGD sono assegnati i compiti riportati nell'***Allegato 13***, prescritti dalla normativa vigente e richiesti per l'operatività funzionale della gestione documentale di cui al presente Manuale. L'allegato è suscettibile di modifica in caso di variazioni normative e/o organizzative del Consiglio regionale della Puglia deliberate dagli Organi competenti e/o dalla funzione di governo dell'Amministrazione.

Articolo 7 - Accreditamento dell'Amministrazione/AOO all'IPA

Il Consiglio regionale della Puglia, nell'ambito degli adempimenti correnti, ha provveduto ad accreditarsi presso l'Indice delle Pubbliche Amministrazioni (IPA) conservato e pubblicato dall'agenzia per l'Italia Digitale (AgID), fornendo le seguenti informazioni identificative:

- denominazione della amministrazione;
- codice fiscale dell'Amministrazione;
- indirizzo della sede principale dell'Amministrazione;
- nominativo del referente dell'Amministrazione per l'IPA;
- codice identificativo proposto per la amministrazione;
- denominazione e codice identificativo dell'AOO;
- casella di posta elettronica certificata dell'AOO direttamente associata al registro di protocollo;
- caselle di posta elettronica certificata dell'AOO direttamente associate al registro di protocollo, che trattano peculiari tipologie di documenti;
- il nominativo del responsabile della gestione documentale;
- la data di istituzione;
- l'eventuale data di soppressione;
- l'elenco degli uffici utente dell'area organizzativa omogenea e loro codici identificativi.

Le informazioni inerenti l'Amministrazione sono riportate in ***Allegato 6***.

L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il sito www.indicepa.gov.it da parte di tutti i soggetti pubblici o privati.

L'Amministrazione, attraverso il RGD o il suo VIC comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data di entrata in vigore delle

stesse in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; analogamente l'Amministrazione comunica la soppressione ovvero la creazione di una nuova AOO nella forma dovuta. Gli aggiornamenti delle predette informazioni avvengono mediante l'utilizzo dei servizi telematici offerti dall'IPA e con le modalità operative di cui all'***Allegato 19***.

Articolo 8 - Caselle di Posta Elettronica

L'AOO è dotata delle caselle di Posta Elettronica Certificata (PEC) pubblicate sull'Indice delle Pubbliche Amministrazioni (IPA) direttamente associate al registro di protocollo e distinte per il trattamento di peculiari tipologie di documenti e non.

Inoltre, l'Amministrazione, in attuazione di quanto stabilito dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie - impiego della posta elettronica nelle pubbliche amministrazioni - provvede ad assegnare al personale amministrativo e politico una casella di posta elettronica nominativa e/o funzionale. L'***Allegato 3*** riporta l'elenco delle caselle PEC di cui è dotata l'Amministrazione.

Articolo 9 - Sistema di classificazione dei documenti

Con l'entrata in vigore del protocollo unico è adottato anche un unico *Titolario di classificazione* dell'amministrazione per l'AOO che identifica l'Amministrazione stessa così come previsto dalla normativa e dalla corrente disciplina in materia archivistica (***Allegato 4***).

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

Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro lo smistamento di competenza, sarà, inoltre, predisposto un *prontuario di smistamento* unitamente a quello di classificazione.

Il prontuario è una guida rapida di riferimento, in ordine alfabetico documentale che, sulla base del *titolario*, permette l'immediata individuazione della classificazione e delle competenze.

Articolo 10 - Formazione e conservazione del registro giornaliero di protocollo

La formazione del registro giornaliero di protocollo segue le regole tecniche contenute nell'art. 14 del DPCM 13 novembre 2014 - *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 - Pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015*, ossia mediante la "generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in **forma statica**". La **staticità** del *Registro giornaliero* di *protocollo* è garantita mediante "*l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o*

codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione", come disposto dal DPCM 13 novembre 2014.

Oltre alla caratteristica di **staticità**, il *Registro giornaliero di protocollo* possiede le caratteristiche di **immodificabilità** e di **leggibilità**, garantite dall'utilizzo di un formato approvato da organismi internazionali che definiscono la normazione tecnica (quali ISO, CEN, ECM, W3C, etc.) e di **integrità**, garantito dal trasferimento nel Sistema di Conservazione. In ***Allegato 15*** sono riportate le modalità di produzione e di conservazione del *Registro giornaliero di protocollo*, ovvero le modalità per garantire le caratteristiche di staticità, immodificabilità, integrità e leggibilità del registro.

Articolo 11 - Firma digitale

Per l'espletamento delle attività istituzionali, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla. Nell'***Allegato 16*** viene riportato l'elenco delle persone titolari ed assegnatarie di firma digitale ed il loro campo di applicazione.

Articolo 12 - 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 assolve integralmente il dettato del D.lgs. 30 giugno 2003 n.196 con atti formali interni ed esterni.

Riguardo agli adempimenti interni specifici, gli addetti destinati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, vengono delegati dal titolare dei dati e, se nominato, dal Responsabile,

In merito agli adempimenti esterni, l'amministrazione:

- si organizza 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 legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite;
- provvede, in caso di richiesta di accesso diretto ai propri archivi, a rilasciare all'Amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente;
- provvede, in attuazione al Codice sulla Privacy: **per la posta in arrivo o in ingresso** contenente dati personali oggetto di privacy, la UOP della struttura amministrativa competente alla quale viene assegnato l'atto, comunica con immediatezza alla UOPG i livelli di autorizzazione verticale specificando il personale o la struttura abilitate alla sola visione e/o all'inserimento ed alla modifica delle informazioni; **per la posta in partenza o in uscita** ogni struttura incaricata al protocollo provvede a definire l'oggetto secondo le modalità previste dal Codice della Privacy e ad inserire solo gli allegati che non comportano violazione delle norme sul trattamento dei dati. Contemporaneamente

provvede ad inserire nel sistema il personale e/o le classi omogenee incaricate ad accedere, visualizzare e/o abilitate all'inserimento ed alla modifica delle informazioni.

Nel caso di **atti in uscita dal protocollo generale**, la struttura mittente deve esplicitamente indicare, con nota a parte, quale posta sia soggetta al trattamento di riservatezza fornendo al servizio protocollo tutte le indicazioni di cui al punto precedente.

La mancata o non corretta applicazione della procedura indicata resta nella responsabilità della UOP e/o della struttura competente come sopra individuata.

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

Alla protezione dei dati personali trattati all'interno dell'Amministrazione si è provveduto ai sensi del dettato delle norme del D.lgs. 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 requisiti dei dati;
- all'informativa fornita agli interessati ed al consenso quando dovuto;
- alla nomina degli incaricati del trattamento per gruppo o individualmente;
- alle misure minime di sicurezza.

Articolo 13 - Formazione

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

In particolare, considerato che il personale assegnato agli UOP deve conoscere:

- l'organizzazione ed i compiti svolti da ciascun UOR all'interno della AOO,
- gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni,
- le modifiche introdotte dal DPCM 3 dicembre 2013 - *Regole Tecniche per il protocollo informatico* - e l'impatto nei processi organizzativi interni,

sono stati previsti specifici momenti formativi volti ad assicurare la formazione e l'aggiornamento professionale in termini di conoscenza:

- relativa ai processi di semplificazione ed alle innovazioni procedurali inerenti la protocollazione e l'archiviazione dei documenti della AOO,
- di strumenti e tecniche per la gestione digitale delle informazioni, con particolare riferimento alle politiche di sicurezza stabilite dall'amministrazione/AOO,
- delle norme sulla protezione dei dati personali e delle direttive stabilite nel documento programmatico della sicurezza.

Tali azioni formative, soggette a revisione annuale, destinati a operatori, funzionari e dirigenti sono riportati in ***Allegato 5***.

Articolo 14 - Sorgente interna dei documenti

Per *direzione* INTERNA dei documenti si intende qualunque RPA che invia formalmente della corrispondenza alla propria UOP, ovvero alla UOPG nel caso di assenza di una propria UOP, per essere protocollata e trasmessa, nelle forme opportune, ad altra RPA o UOR della stessa AOO.

Per documento in partenza s'intende il documento con rilevanza giuridico-probatoria o costitutiva prodotto dal personale dell'AOO nell'esercizio delle proprie funzioni.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti titoli. I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nell'articolo 35-posta elettronica certificata.

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

Nei documenti in partenza viene specificato che il destinatario è tenuto a citare i riferimenti di protocollo della lettera cui fa riscontro.

Durante la fase transitoria di migrazione verso il sistema di gestione documentale interamente digitale, il documento può essere anche in formato analogico. I mezzi di recapito della corrispondenza considerati in questo caso sono il servizio postale, nelle sue diverse forme, ed il servizio telefax/server fax.

Articolo 15 - Verifica formale dei documenti

Ogni UOP è autorizzata dall'AOO per il tramite del RGD, a svolgere attività di protocollazione e segnatura sulla corrispondenza in uscita e, in particolari situazioni di emergenza e/o necessità, anche in arrivo, dal proprio ambito.

Di conseguenza tutti i documenti originali da spedire, siano essi in formato digitale o analogico, vengono direttamente protocollati, "segnati" e:

- Trasmessi, nelle forme opportune, al/ai destinatario/i, se trattasi di documenti con direzione INTERNA;
- Inviati alla UOPG per la trasmissione, nelle forme opportune, al/ai destinatario/i, se trattasi di documenti con direzione IN USCITA;

Articolo 16 - Trasmissione di documenti cartacei a mezzo posta

L'affrancatura della posta in partenza è consentita per la sola trasmissione della corrispondenza avente carattere istituzionale e d'ufficio, regolarmente protocollata secondo il SPG. Resta, pertanto, esclusa dall'affrancatura tutta la corrispondenza non rientrante in tale tipologia (ad esempio auguri, cordogli ecc. che non hanno valenza istituzionale).

Per quanto concerne i Gruppi consiliari gli stessi provvedono direttamente alla spedizione in quanto dotati di apposito capitolo di spesa.

Al riguardo si rammenta che la trasmissione per posta, con relativa affrancatura, di documenti analogici va fatta solo nei casi in cui non sia possibile la trasmissione per via telematica (PEC, PE, FAX, VoIP, ecc.) restando le responsabilità previste a carico del soggetto richiedente (cfr. normativa sul contenimento delle spese postali: vedi: art. 63, comma 3bis, del D. Lgs n. 82 del 7.3.05; art. 76 Legge Finanziaria 2008 e successive; comma 1 ter dell'art. 12 (CAD); ecc).

La singola UOP, dopo la protocollazione e la "segnatura", provvede direttamente alla trasmissione "fisica" dei documenti in partenza, alla UOPG, alle cui competenze è assegnato l'ufficio posta centralizzato, abilitato alla spedizione "fisica" della corrispondenza.

Per quanto concerne la spedizione di posta avente destinazione esterna alla sede del Consiglio e soggetta ad affrancatura, le operazioni di consegna al relativo servizio postale devono avvenire entro e non oltre le ore 11,00 di ogni giorno lavorativo, affinché si possa consentire la spedizione nella stessa giornata. La posta in partenza consegnata oltre le ore 11,00 verrà spedita il giorno successivo.

Al fine di rendere efficiente il servizio anche per eventuali ricerche e verifiche di spedizioni, ogni struttura accompagnerà la propria posta in partenza da una distinta di spedizione e provvederà, altresì, ad indicare sulla busta il relativo protocollo.

Ogni Struttura del Consiglio ha a disposizione, presso l'ufficio Posta sito al V° piano del palazzo in Via Capruzzi, una cassetta postale nella quale è depositata la Posta in arrivo dall'esterno. La posta deve essere prelevata, almeno una volta ogni giorno lavorativo, a cura del personale formalmente incaricato da ciascuna struttura del Consiglio.

Articolo 16.1 Affrancatura dei documenti in partenza

L'UOPG *(tramite l'ufficio posta centrale)* provvede, sulla base delle regole dettate dagli operatori postali, alle operazioni propedeutiche l'affrancatura della corrispondenza in partenza comprensive di:

- verifica per l'affrancatura delle lettere ordinarie come posta prioritaria;
- ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici;
- registrazioni della corrispondenza in partenza distinta per tipologia: posta prioritaria, raccomandate e raccomandata A.R., raccomandate estere, pacchi e/o plichi ecc.

Al fine di consentire il regolare svolgimento delle operazioni di cui al comma precedente, la corrispondenza in partenza deve essere conferita alla UOP (o in alternativa all'ufficio posta), accompagnata da una distinta riepilogativa, secondo le regole richiamate nel precedente articolo 35, opportunamente confezionata, in busta chiusa che deve riportare in modo chiaro: il destinatario con tutte le informazioni di rito (indirizzo, CAP, ecc.); il mittente ed il numero di protocollo del documento che viene trasmesso.

Articolo 16.2 Conteggi spedizione corrispondenza

L'UOPG (*tramite l'ufficio posta*) provvede ad effettuare le verifiche dei conteggi relativi alle spese per la posta in partenza nel modo che segue:

- verifiche giornaliere, settimanali e mensili delle spese per l'affrancatura, sui modelli utilizzati per la spedizione e completati dalla azienda fornitrice del servizio nella parte relativa all'effettivo costo sostenuto e calcolato in base ai contratti stipulati;
- raccolta e catalogazione dei modelli delle spese di affrancatura per singoli mesi in ogni anno solare.

Articolo 16.3 Documenti in partenza per posta convenzionale con più destinatari.

Qualora i destinatari siano diversi è consentita la spedizione di copie dell'originale.

L'elenco dei destinatari, in formato cartaceo, viene allegato alla minuta.

Articolo 17 - Trasmissione di documenti cartacei a mezzo fax

Sul documento trasmesso via fax occorre apporre la dicitura: "**Si invia solo per FAX ai sensi del D.Lvo n. 82/2005 e s.m. – Non segue trasmissione in formato cartaceo**"

Solo se esplicitamente richiesto dal destinatario verrà trasmesso l'originale.

Nel caso di più destinatari si provvede ad invii successivi o in un'unica modalità se l'apparecchiatura FAX/ServerFAX consente la trasmissione multipla.

Le ricevute, a certificazione della avvenuta trasmissione, vengono allegate al documento originale come indicato nel successivo articolo 36.1.

Articolo 17.1 Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi FAX/ServerFAX di corretta trasmissione, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, viene conservata all'interno del relativo fascicolo.

Le UOP di protocollo che effettuano la spedizione di documenti informatici o cartacei curano anche l'invio delle ricevute di ritorno al mittente che si fa carico di archiviarle nel relativo fascicolo logico o fisico.

Articolo 18 - Orari di accesso alla struttura di protocollo e spedizione posta

Al fine di consentire il regolare funzionamento della struttura e la possibilità di effettuare l'attività di registrazione e spedizione entro la stessa giornata, fatto salvo i casi eccezionali in analogia a quanto previsto nel precedente articolo 16, l'accesso alla struttura di protocollo è consentito al personale autorizzato ed agli utenti interni e/o esterni per il solo tempo necessario al deposito/consegna degli atti da registrare e, precisamente:

- Per tutti i giorni lavorativi in orari antimeridiani dalle ore 09:00 alle ore 13:00;
- Per le giornate di martedì e giovedì in orari pomeridiani dalle ore 14:30 alle ore 17:00
- Nelle giornate di lunedì, mercoledì e venerdì dalle ore 14:30 alle ore 16:00 sulla base dell'assegnazione dello straordinario.

Conseguentemente la Sezione Informatica e Tecnica all'inizio di ogni anno provvederà a modificare/ridefinire il relativo orario generale di apertura del protocollo.

Per particolari necessità il dirigente della Sezione Informatica e Tecnica può consentire l'accesso in deroga agli orari sopra stabiliti.

Il personale addetto provvede alla registrazione e spedizione della corrispondenza seguendo l'ordine di arrivo e/o deposito della stessa presso la struttura, fatto salvo per gli atti urgenti che vengono protocollati e/o trasmessi con immediatezza.

L'indicazione d'urgenza è affidata alla valutazione del responsabile del protocollo della Sezione Informatica e Tecnica sentito, se necessario, il proprio dirigente di riferimento.

TITOLO III ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

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

Articolo 19 - Piano di attuazione

In coerenza con quanto già in atto dal 01.01.2004 tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico.

Pertanto tutti gli altri registri di protocollo sono stati aboliti ed eliminati.

Tutti i protocolli di settore e di reparto, di telefax e più in generale i protocolli diversi dal protocollo informatico previsto nel Testo unico sono stati eliminati, salvo eventuali verifiche locali da svolgere da parte del RGD, entro e non oltre **tre mesi** dall'entrata in vigore del presente MdG.

TITOLO IV PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

Il *Piano per la Sicurezza Informatica* del Consiglio regionale della Puglia rev. 2015/A01 del 12/10/2015, data la necessaria riservatezza da dare al documento, è conservato agli atti del Sezione Informatica e Tecnica.

Di seguito sono riportate le caratteristiche generali del *Piano di Sicurezza,* mentre nell'***Allegato 17*** è riportato un estratto del Piano rev. 2015/A01 del 12/10/2015.

Articolo 20 - Definizione

Il *Piano per la Sicurezza Informatica* riporta le misure di sicurezza adottate per la *formazione*, la *gestione*, la *trasmissione*, *l'interscambio*, l'*accesso* e la *conservazione* dei documenti informatici, nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del Decreto Legislativo del 30 giugno 2003, n. 196 e successive modificazioni.

Articolo 21 - Obiettivi del Piano di sicurezza

Il *Piano di Sicurezza* garantisce che:

- i documenti e le informazioni trattate dall'AOO siano *disponibili, integre* e *riservate*;
- 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.

Articolo 22 - Redazione e revisioni

Il *Piano di Sicurezza* è redatto e aggiornato d'intesa con il *Team per la Sicurezza Informatica* (composto da: Dirigente del Sezione Informatica e Tecnica, Responsabile della Gestione Documentale, Vicario del Responsabile della Gestione Documentale, Responsabile del Trattamento dei dati personali, Amministratore di Sistema e Project Leader del Sistema di Protocollazione).

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo e di assistenza sistemistica, gran parte delle funzioni/responsabilità di sicurezza informatica sono demandate ai Fornitori dei suddetti servizi (Project Leader del Sistema di Protocollazione e Amministratore di Sistema esterno). All'AOO, in quanto fruitrice dei servizi, sono demandate le componenti "*locali*" della sicurezza e del controllo, poiché attraverso la propria organizzazione, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "*valore*" dei dati/documenti trattati.

Il *Piano di Sicurezza*:

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

Il *Piano di Sicurezza* è soggetto a revisione formale con cadenza almeno **biennale**. Esso può comunque essere **modificato** ogni volta si renda necessario a seguito di eventi gravi o di variazioni sostanziali dell'infrastruttura telematica.

Articolo 23 - Misure di sicurezza per la formazione dei documenti informatici

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

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

I documenti informatici dell'AOO sono prodotti con l'ausilio di applicativi di *office automation* in grado di generare formati che siano standard internazionali (*de jure e de facto*) e che, quindi, garantiscono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Considerata l'evoluzione tecnologica e l'elevato grado di obsolescenza, nell'***Allegato 18*** è riportato l'elenco dei formati adottati dal Consiglio regionale della Puglia per la formazione, gestione e conservazione dei documenti informatici.

Articolo 24 - Misure di sicurezza per la gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico in modalità client/server ed in modalità WEB è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo dei server che ospitano i data base dei documenti protocollati e le loro informazioni è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa 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 giornaliero di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata, interni 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.

Articolo 24.1 Componente organizzativa della sicurezza

La componente organizzativa della sicurezza è legata al sistema informatico in uso per la gestione del protocollo e della documentazione e, quindi, è demandata alle attività richieste alla Società affidataria per la fornitura e manutenzione del SdP.

Pertanto nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, la Società affidataria del SdP, dovrà prevedere le seguenti **funzioni specifiche** minime:

- *sicurezza informatica:-* definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza. Contribuisce alla definizione delle linee strategiche di sicurezza dell'Amministrazione;
- *sicurezza operativa:-* realizzazione, gestione e manutenzione in efficienza delle misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dall'Amministrazione;
- *revisione:-* controllo che le misure di sicurezza adottate siano efficaci e coerenti con le linee strategiche di indirizzo definite dall'Amministrazione.

Articolo 24.2 Componente fisica della sicurezza

Le dotazioni informatiche di governo e memorizzazione dati sono ubicate nella *Sala Server Principale* del Consiglio. Il controllo degli accessi fisici alla Sala Server è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione prevista nel *Piano di Sicurezza*. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati dal personale della Sezione Informatica e Tecnica del Consiglio e/o da suoi delegati;
- ogni persona che accede alle risorse della *Sala Server Principale* del Consiglio deve essere identificata in modo certo, anche con sistemi di autenticazione forte;
- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati.

Articolo 24.3 Componente logica della sicurezza

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

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

- l'attivazione dei servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico;
- l'identificazione, l'autenticazione e l'autorizzazione degli addetti della AOO alle attività di protocollazione e gestione documentale attraverso il SdP;
- la riservatezza dei dati;
- l'integrità dei dati;
- l'integrità del flusso dei messaggi;
- il non ripudio dell'origine (da parte del mittente);
- il non ripudio della ricezione (da parte del destinatario);
- l'audit di sicurezza;
- la ridondanza dei sistemi di esercizio.

Articolo 24.4 Componente infrastrutturale della sicurezza

Presso la *Sala Server Principale* del Consiglio sono disponibili i seguenti impianti:

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

Essendo la *Sala Server Principale* del Consiglio lontano da insediamenti industriali e posta 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.

Articolo 24.5 Gestione delle registrazioni di sicurezza

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

Le registrazioni di sicurezza sono costituite:

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

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 del servizio di protocollo;
- le registrazioni del SdP sono elaborate tramite procedure automatiche da parte degli operatori e sono soggette a conservazione secondo quanto previsto dalle *Regole tecniche per la Conservazione*;
- 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/cassaforte ignifugo nell'Ufficio della AP Responsabile dei sistemi informatici e tecnici;
- i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica.

Articolo 25 - Misure di sicurezza per la trasmissione e l'interscambio dei documenti informatici

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

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

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

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

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

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

Articolo 25.1 Interscambio con altre AOO

Come previsto all'art. 16, co. 1, delle Regole Tecniche, lo scambio dei documenti soggetti alla registrazione di protocollo con altre AOO è effettuato mediante messaggi di Posta Elettronica Certificata. Il SdP provvede a gestire automaticamente la trasmissione/ricezione del documento informatico interfacciandosi con il sistema di Posta Certificata in uso presso il Consiglio regionale della Puglia. Per i messaggi scambiati all'esterno della AOO con la Posta Elettronica Certificata non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza.

Articolo 25.2 Interscambio all'interno della AOO

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

Gli uffici organizzativi di riferimento (UOR) dell'AOO si scambiano documenti informatici attraverso l'utilizzo del SdP e/o delle caselle di posta elettronica.

Articolo 26 - Accesso ai documenti informatici

Il controllo degli accessi ai documenti informatici è assicurato utilizzando un sistema di autenticazione a singolo fattore: una parola chiave (*password – ciò che so*) assegnata al codice identificativo personale (*username*) 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 gruppo di utenti o ad un singolo utente del Sistema di protocollo e

gestione documentale. Queste, in sintesi, sono:

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

Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori dell'AOO che per gli utenti dell'AOO ed interessano tutti i sistemi informativi del Consiglio.

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

Il SdP in uso nell'AOO:

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

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

Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

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

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

Articolo 26.1 Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RGD dell'AOO di concerto con il Dirigente del Servizio Informatico e Tecnico. Tali livelli si distinguono in:

- abilitazione alla consultazione,
- abilitazione all'inserimento,
- abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta

esplicita del DSIT o per errori di inserimento);

- le credenziali private degli utenti e dell'Amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né, successivamente, al momento del login.

Articolo 26.2 Accesso al registro di protocollo per utenti interni alla AOO

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

- liste di competenza, gestite dall'amministratore di AOO, per la definizione degli utenti abilitati ad accedere a determinate voci del titolario;
- ruoli degli utenti, autorizzati dal DSIT e gestita dall'Amministratore di sistema, per la specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "particolare o riservata", autorizzati dal DSIT e gestita dall'Amministratore di sistema, 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 Gestione Documenti" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.

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

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

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

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

Articolo 26.3 Utenti esterni alla AOO - Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al Capo VIII del Nuovo CAD, è allo studio.

Articolo 26.4 Utenti esterni alla AOO - Privati

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

Articolo 27 - Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 – *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005* - pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015.

Le modalità di conservazione dei documenti informatici del Consiglio sono riportate nell'***Allegato 20***.

GESTIONE DEI FLUSSI DOCUMENTALI

Articolo 28 - Flussi documentali in ingresso

Tutti i documenti trattati dall'Amministrazione - in ingresso o a circolazione interna e indipendentemente dal supporto sul quale sono formati - devono di regola essere protocollati con sistema informatizzato che ne consente l'immediata tracciabilità e reperibilità, ad eccezione di quelli di cui al successivo Articolo 31 -.

La gestione della documentazione ricevuta dall'AOO si svolge secondo le seguenti fasi:

1) Ricezione
2) Protocollazione
3) Segnatura
4) Assegnazione

Articolo 28.1 *Ricezione*

I documenti possono pervenire all'AOO:

- in forma digitale (*documenti informatici*);
- in forma cartacea (*documenti analogici*).

Articolo 28.1.1 Documenti informatici

Per documento informatico s'intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, come definito all'Art. 1 comma 1 lettera *p)* del *Nuovo CAD*.

L'Amministrazione assicura l'accettazione dei documenti elettronici inviati ai suoi uffici tramite gli indirizzi di posta elettronica e/o di posta elettronica certificata riportati sul sito dell'IPA, servizi telematici o consegnati su supporto digitale, quando prodotti in uno dei formati di cui all'***Allegato 18*** del presente Manuale.

Laddove, invece, il documento inviato o consegnato agli uffici dell'AOO sia prodotto in un formato diverso da quello previsto nel presente Manuale e tale da non consentirne una corretta gestione, l'ufficio competente ne darà comunicazione al mittente richiedendo contestualmente la ripetizione dell'invio in uno dei formati indicati nell'elenco ovvero in altro formato concordato con l'ufficio.

Articolo 28.1.2 Documenti analogici (cartacei)

Per documento analogico s'intende la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti, come definito all'Art. 1 comma 1 lettera *p-bis)* del *Nuovo CAD* e sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, quali:

- posta pervenuta per il tramite di Poste italiane S.p.A. e/o di altri gestori autorizzati,
- posta pervenuta attraverso il servizio di consegna interno;
- posta recapitata direttamente (*brevi manu*);

- posta ricevuta via fax/server fax.

Articolo 28.2 Protocollazione

La registrazione dei documenti in ingresso è assicurata dalla UOPG e dalle UOP con l'ausilio delle funzionalità del SdP.

Le registrazioni di protocollo generale sono eseguite in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni fondamentali - data e numero di protocollo, oggetto, generalità del mittente e/o destinatario - in più fasi successive.

Ciascuna registrazione di protocollo, ai sensi dell'art. 53 del DPR n. 445/2000, contiene dati obbligatori e dati accessori.

Elementi obbligatori	
Documenti in Arrivo	Documenti in Partenza
• numero protocollo • data registrazione • mittente/i • oggetto del documento • impronta del documento (se informatico) • data e n. protocollo mittente se disponibili	• numero protocollo • data registrazione • destinatario/i • oggetto del documento • impronta del documento (se informatico)

Elementi accessori
• numero degli allegati • descrizione degli allegati • estremi dell'autorizzazione al differimento dei termini di registrazione; • mezzo di ricezione o di spedizione; • unità organizzativa cui il documento è assegnato per competenza; • unità organizzative alle quali il documento è assegnato per conoscenza; • tipo di documento.

La numerazione delle registrazioni di protocollo è unica per tutte le strutture che compongono l'AOO ed è rigidamente progressiva.

La numerazione si chiude il **31 dicembre** di ogni anno e viene rinnovata all'inizio di ogni anno solare.

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

Il numero di protocollo è costituito da almeno sette cifre numeriche, ai sensi dell'articolo 57 del DPR n. 445/2000.

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.

La documentazione che non è stata registrata presso una UOP e/o presso la UOPG viene considerata giuridicamente inesistente presso l'Amministrazione.

Non è consentita la protocollazione di un documento che sia già stato protocollato.

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

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

Articolo 28.3 Segnatura di protocollo dei documenti

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

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

Essa consente di individuare ciascun documento in modo inequivocabile.

La segnatura è posta, di norma, sul fronte del documento in arrivo attraverso etichetta o con apposito timbro, come riportato in ***Allegato 9***.

Articolo 28.4 Assegnazione

Dopo essere stato sottoposto a registrazione di protocollo, ogni documento viene assegnato alla/e struttura/e di competenza per il successivo trattamento utilizzando le funzionalità del sistema SdP in uso e meglio specificate nell' ***Allegato 8***.

Nel caso di assegnazione non corretta, l'Ufficio che riceve il documento lo restituisce, motivando la restituzione, alla struttura assegnante, che provvederà ad assegnarlo nuovamente.

Articolo 29 - Flussi documentali in uscita

Il ciclo di produzione dei documenti destinati all'uscita dall'AOO prevede le seguenti fasi di lavorazione:

1) Formazione del documento
2) Sottoscrizione
3) Registrazione di protocollo
4) Spedizione

Articolo 29.1 Formazione del documento

I documenti in uscita dall'AOO possono essere prodotti:

- mediante strumenti informatici di elaborazione di testi;

- mediante applicazioni informatizzate che curano determinati procedimenti amministrativi e producono automaticamente gli atti destinati alla notifica o alla spedizione.

Articolo 29.2 Sottoscrizione

Completata la fase di redazione, il documento viene sottoscritto da colui che è titolare del potere di firma o da un suo delegato, alternativamente:

- con **firma autografa**, quando l'originale del documento è prodotto in forma cartacea;
- con **firma digitale**, nel caso in cui il documento originale sia prodotto in forma elettronica.

Eventuali deleghe di firma, in forza delle quali la sottoscrizione può essere curata da un soggetto diverso dal titolare del potere di firma, devono risultare da uno specifico atto emanato dal responsabile dell'AOO e conservato agli atti dell'ufficio.

Nel caso in cui la sottoscrizione di un documento avvenga sulla base di una delega, di questa dovrà esserne fatta menzione nel documento, eventualmente anche riportando gli estremi identificativi dell'atto di cui al paragrafo precedente.

Articolo 29.3 Registrazione di protocollo

Tutti i documenti in uscita dall'AOO devono essere registrati, dopo la sottoscrizione, nel Registro Ufficiale di Protocollo.

Ogni registrazione di protocollo deve identificare un solo documento, pertanto non è possibile attribuire a un documento in uscita lo stesso numero di protocollo attribuito all'eventuale documento in entrata dal quale è scaturita la lavorazione.

Articolo 29.4 Spedizione

Un documento sottoscritto e protocollato viene inviato al destinatario utilizzando uno dei possibili canali di spedizione disponibili.

Per i documenti registrati sul Registro ufficiale di protocollo, il canale utilizzato per l'invio al destinatario viene annotato sul sistema SdP al momento della protocollazione in uscita.

Articolo 29.5 Utilizzo del fax tra pubbliche amministrazioni

A norma dell'art. 14 del decreto-legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98 è escluso l'uso del fax per lo scambio di documenti tra pubbliche amministrazioni, mentre non vi sono preclusioni normative per lo scambio di documentazione tra pubbliche Amministrazioni e cittadini o imprese.

Articolo 30 - Flussi documentali interni all'AOO

I documenti scambiati tra uffici interni della AOO non sono soggetti all'obbligo di registrazione sul Registro Ufficiale di Protocollo, lasciando tale facoltà in capo a ciascun Responsabile.

Comunque per poter mantenere la tracciabilità dei documenti oggetto di scambio tra le strutture interne all'AOO, viene utilizzato il Registro Ufficiale di Protocollo.

I documenti registrati con direzione INTERNO seguono le stesse fasi di assegnazione previste all'*Articolo 28.4*. nonché di quanto indicato nel seguente *Articolo 31* in merito ai documenti non soggetti a protocollazione..

Articolo 31 - Documenti da non sottoporre a registrazione obbligatoria nel protocollo generale

Sono esclusi dalla protocollazione, ai sensi dell'art. 53 del DPR n. 445/2000, in quanto soggetti a sistema di **registrazione diversificata**, i documenti di cui all'***Allegato 7***.

Articolo 32 - Registro giornaliero di protocollo

Il RGD 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, alla produzione del pacchetto di versamento secondo quanto stabilito dall'art. 7 del DPCM 13 novembre 2014, firmarlo digitalmente ed effettuare la trasmissione e la verifica nel sistema di conservazione, così come riportato nell'***Allegato 15***.

Articolo 33 - Annullamento delle registrazioni di protocollo

La modifica anche di un solo campo – *tra quelli obbligatori della registrazione di protocollo, compilato dall'operatore o in modo automatico dal sistema e registrate in forma non modificabile* – che si rendesse necessaria per correggere errori intercorsi in sede di immissione di dati comporta l'annullamento "d'ufficio" e contestuale nuova e completa registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullate 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.

In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

L'annullamento della registrazione di protocollo generale viene richiesto con specifica nota, adeguatamente motivata, indirizzata al RGD.

A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.

Il registro indica i motivi dell'annullamento e, se il documento è stato riprotocollato, il nuovo numero di protocollo assegnato.

Invece l'annullamento anche di un solo campo - *tra quelli non obbligatori per la registrazione di protocollo* - necessario per correggere errori intercorsi in sede di immissione dati di altre informazioni, può essere effettuata attraverso il SdP, che provvede a tenere traccia sia temporale che contenutistica degli interventi effettuati.

Non è possibile annullare protocolli di atti già trasmessi attraverso il SdP o spediti all'esterno. In tali casi, va redatta specifica nota che provvede ad annullare, sostituire, modificare o integrare l'atto di che trattasi. L'UOP provvede ad inserire il n° di protocollo nella Sezione "collegati" del SdP al fine di consentirne la tracciabilità.

In ***Allegato 20*** sono riportate le modalità operative di modifica informazioni o annullamento protocollo.

Articolo 34 - Gestione delle registrazioni di protocollo con il SdP

La produzione delle registrazioni di protocollo informatico, l'operazione di "segnatura" delle stesse e le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono demandate al SdP.

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

Articolo 35 - Il registro di emergenza

Qualora non fosse disponibile fruire del SdP per interruzione accidentale o programmata, l'Amministrazione/AOO effettua le registrazioni di protocollo sul registro di emergenza.

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

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

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

Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo generale.

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

A tale registrazione viene associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

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

L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza a cui viene fatto riferimento per l'avvio dei termini del procedimento amministrativo.

L'efficienza, invece, è garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica.

Pertanto il RGD autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su un registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il Sistema.

Nella condizione di emergenza si applicano le seguenti modalità di registrazione e di recupero dei dati:

a) sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;

b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il RGD può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;

c) per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;

d) la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve essere unica per ciascun anno e deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea;

e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

TITOLO V CLASSIFICAZIONE, FASCICOLAZIONE E ARCHIVIAZIONE DEI DOCUMENTI

Articolo 36 - Titolario di classificazione

Con l'entrata in vigore del protocollo unico è adottato anche un unico *Titolario di classificazione* dell'amministrazione per l'AOO che identifica l'Amministrazione stessa così come previsto dalla normativa e dalla corrente disciplina in materia archivistica (***Allegato 4***).

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

Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro lo smistamento di competenza, sarà, inoltre, predisposto un *prontuario di smistamento* unitamente a quello di classificazione.

Il prontuario è una guida rapida di riferimento, in ordine alfabetico documentale che, sulla base del *Titolario*, permette l'immediata individuazione della classificazione e delle competenze.

Il Titolario di classificazione è mantenuto aggiornato dal Responsabile della gestione documentale.

ARTICOLO 36.1 Attribuzione del codice di classificazione ai documenti

Tutti i documenti (anche quelli non protocollati) sono soggetti a classificazione.

La classificazione di un documento avviene associando ad esso almeno una voce del Titolario di classificazione individuando quella più opportuna a identificare il documento tra quelle disponibili.

Nel caso in cui da uno stesso documento scaturiscano più attività di natura diversa, è possibile associare al documento più voci di classificazione in funzione delle attività nell'ambito delle quali il documento viene trattato.

La classificazione può anche avvenire successivamente al momento della protocollazione e in ogni momento della lavorazione è possibile modificare o integrare la classificazione già apposta ad un documento. Spetta all'addetto al quale il documento è assegnato per la lavorazione verificare la correttezza della classificazione e, se necessario, modificarla di conseguenza.

In ogni caso, la classificazione deve essere effettuata prima della conclusione della lavorazione.

Articolo 37 - Fascicolazione dei documenti

I documenti ricevuti e prodotti dagli uffici dell'AOO sono raccolti in fascicoli costituiti in modo che ciascuno rappresenti l'insieme ordinato dei documenti riferiti ad uno stesso procedimento amministrativo o, comunque, ad una stessa pratica.

I fascicoli possono essere:

- *Fascicoli cartacei:* tutta la documentazione originale della pratica è prodotta in formato cartaceo;
- *Fascicoli informatici:* tutta la documentazione originale della pratica è prodotta in formato elettronico;
- *Fascicoli misti:* la documentazione riguardante la pratica è formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico. In questi casi vengono prodotti due fascicoli distinti:
  - un fascicolo cartaceo nel quale viene raccolta la documentazione cartacea;
  - un fascicolo informatico, archiviato nel sistema di gestione documentale, nel quale sono raccolti tutti i documenti prodotti in formato elettronico e i riferimenti di protocollo dei documenti prodotti in formato cartaceo.

  I due fascicoli sono collegati tra loro e i riferimenti al fascicolo collegato sono riportati sia nella copertina del fascicolo cartaceo che nei dati di identificazione del fascicolo informatico.

I fascicoli possono essere distinti nelle seguenti tipologie:

- Fascicoli per processo/procedimento, contenenti tutti i documenti ricevuti, inviati o interni afferenti una stessa "pratica";
- Fascicoli per serie documentale, in cui vengono aggregati documenti della stessa tipologia.

I Responsabili degli Uffici interni all'AOO, nell'ambito dei principi contenuti nel presente Manuale, forniscono le indicazioni operative per la gestione dei fascicoli a coloro che curano le relative pratiche e assicurano che la costituzione dei fascicoli avvenga secondo modalità uniformi per tutta l'AOO, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco (ad es. partita IVA/codice fiscale del fornitore, anno di esercizio contabile, tesoreria, etc.) che di quelli adottati per la descrizione del fascicolo (elenco forniture, note di intervento, pagamenti cedolini, etc.).

I fascicoli sono conservati, fino al versamento nell'archivio di deposito o nel sistema di conservazione, presso gli Uffici che curano le relative pratiche.

Entro i termini previsti per la conservazione a norma, i fascicoli sono versati nell'archivio di deposito o nel sistema di conservazione secondo le modalità descritte nel Manuale della Conservazione.

Articolo 38 - Archiviazione dei documenti

Ai fini di un corretto esercizio dell'azione amministrativa, i fascicoli prodotto dagli uffici dell'AOO sono raccolti in archivi che possono essere distinti in:

- *archivio corrente*, la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione;

- *archivio di deposito*, la parte di documentazione di affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso.

Per i documenti e i fascicoli informatici l'archiviazione corrente si identifica con l'archiviazione all'interno del sistema SdP di gestione documentale.

ARTICOLO 38.1 Archiviazione dei documenti elettronici

Tutti i documenti elettronici pervenuti all'AOO sono acquisiti all'interno del sistema SdP contestualmente alla loro protocollazione.

Analogamente, i documenti elettronici prodotti all'interno dell'AOO sono acquisiti all'interno del sistema SdP quando:

- *siano stati associati (come documento principale o come allegato) ad un protocollo in uscita;*
- *siano stati associati (come documento principale o come allegato) ad un registrazione su un registro interno;*
- *siano stati inseriti in un fascicolo elettronico.*

In tutti i suddetti casi, l'acquisizione all'interno del sistema ne garantisce l'archiviazione.

ARTICOLO 38.2 Archiviazione dei documenti cartacei

Fino alla completa adozione di una gestione documentale in forma elettronica sia per i documenti in ingresso che per quelli in uscita, l'archiviazione dei documenti cartacei avverrà secondo le indicazioni fornite con il presente Manuale.

ARTICOLO 38.3 7.3.3. Piano di conservazione dell'archivio

L'AOO definisce un piano di conservazione dei documenti (c.d. *massimario di scarto*) che stabilisce i tempi di conservazione dei fascicoli e di ciascuna serie documentaria nella loro gestione corrente e di deposito.

Il piano di conservazione individua, per ogni voce di *Titolario*, la documentazione destinata alla conservazione permanente, e quella da proporre per lo scarto.

ARTICOLO 38.4 Versamento dei fascicoli nell'archivio di deposito

L'AOO individua i locali e gli spazi da destinare ad un archivio di deposito (Deposito Archivistico Consiliare). Tale struttura conserva tutti gli atti prodotti in formato cartaceo dai diversi Uffici e non più necessari alle attività amministrative correnti che non siano stati interessati da operazioni di scarto o conferimento agli Archivi di Stato o Regionali.

Periodicamente, gli Uffici individuano i fascicoli che debbono essere versati nel Deposito Archivistico Consiliare.

Il trasferimento deve essere effettuato rispettando l'organizzazione dei fascicoli e delle serie nell'archivio corrente, redigendo un verbale di consegna e curando il trasferimento fisico dei fascicoli.

Il Responsabile del servizio archivistico cura la formazione e la conservazione di un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito consiliare.

Articolo 38.5 Sistema di conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 – *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005* - pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015.

Le modalità di conservazione dei documenti informatici del Consiglio sono riportate nell'***Allegato 20***.

TITOLO VI ALLEGATI AL MANUALE DI GESTIONE DEL DOCUMENTALE DEL CONSIGLIO REGIONALE DELLA PUGLIA