Azienda Pubblica di Servizi alla Persona "Casa Laner"

MANUALE DI GESTIONE PER IL PROTOCOLLO INFORMATICO E L'ARCHIVIO

APPROVAZIONE	MANUALE DI GESTIONE PER IL PROTOCOLLO INFORMATICO E L'ARCHIVIO	REVISIONE 001
Delibera del Consiglio di Amministrazione n. 27 dd. 13/10/2015		**Data della revisione** *08/07/2016*
		Causale della revisione *modifica conservazione*

Sommario

Premessa

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

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto al protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del Titolario di classificazione (allegato 5)e del piano di selezione e di scarto (come previsto da norma di legge);
- 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.

Nel Manuale vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema e vengono descritte le procedure di gestione dei documenti e dei flussi documentali.
Come previsto dalla normativa vigente il presente Manuale di gestione viene reso pubblico attraverso la pubblicazione sul sito istituzionale (www.casalaner.it – sezione "Amministrazione Trasparente"), nello spirito di una piena condivisone degli strumenti di lavoro all'interno della Pubblica Amministrazione, per il raggiungimento dell'obiettivo comune di efficienza e trasparenza nell'azione amministrativa.

TITOLO I
DISPOSIZIONI GENERALI

1.1 AMBITO DI APPICAZIONE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del DPCM 31 ottobre 2000, recante le regole tecniche per il protocollo informatico, nonché ai sensi del D.Lgs. 82/2005 e del DPCM 3 dicembre 2013.
Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'A.P.S.P. "Casa Laner" a partire dal 12 ottobre 2015.
Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.
Il protocollo attesta, anche con effetto giuridico, l'effettivo ricevimento e spedizione di un documento.

1.2 DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:

- per "Amministrazione", l'A.P.S.P. "Casa Laner";
- per "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico;
- per "C.A.D.", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'Amministrazione Digitale.

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

- AOO - Area Organizzativa Omogenea;
- MdG - Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- RSP - Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- RP – Responsabile del protocollo, utente incaricato dal RSP alla tenuta e gestione del protocollo oltre che alla predisposizione del Registro Giornaliero di protocollo;
- RC – Responsabile della conservazione dei Registri giornalieri di protocollo;
- OP – Operatore di protocollo, utente che svolge l'attività di registrazione del protocollo;
- U - Ufficio - 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.

1.3 INDIVIDUAZIONE DELL'AREA ORGANIZZATIVA OMOGENEA

Per la gestione dei documenti, l'Amministrazione individua un'unica AOO che è composta dall'insieme di tutti gli uffici articolati come riportato nell'allegato 1.
L'allegato 1 è suscettibile di modifica in caso di inserimento di nuove AOO/U 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.
All'interno della AOO il sistema di protocollazione è unico. Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
All'interno della AOO il sistema di protocollazione è decentralizzato sia per la corrispondenza in uscita che per la corrispondenza in entrata, attraverso tutti gli U (allegato 8).
Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del RSP.

1.4 SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

Nella 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 RSP.
Al servizio è preposto un dirigente ovvero un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.
L'atto che istituisce il servizio e individua il responsabile della AOO è riportato nell'allegato 2, unitamente:

- al nominativo del RSP;
- al nominativo del vicario del RSP nei casi di vacanza, assenza o impedimento di questi;
- all'elenco dei nominativi degli OP abilitati.

È compito del servizio:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale sul sito internet istituzionale (www.casalaner.it);
- adeguare il documento "Privacy, misure minime della sicurezza e adempimenti D.Lgs 196/2003" in collaborazione con il responsabile della tutela dei dati personali;
- nominare gli OP e definire per ciascuno di essi il tipo di funzione disponibile;
- 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 l'invio del registro giornaliero di protocollo al RC;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- attivarsi affinché le funzionalità del sistema in caso di guasti o anomalie, siano ripristinate entro la tempistica prevista da specifica procedura e, comunque, nel più breve tempo possibile;
- garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- autorizzare gli aggiornamenti del Titolario di classificazione;
- elabora ed aggiorna, nel rispetto della normativa vigente, il Piano di conservazione dei documenti della AOO, integrato con il sistema di classificazione;

- aprire e chiudere il registro di protocollazione di emergenza.

1.5 FIRMA DIGITALE

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.
Nell'allegato 3 viene riportato l'elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione.

1.6 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.
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.
Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel documento "Privacy, misure minime della sicurezza e adempimenti D.Lgs 196/2003".
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.

1.7 CASELLE DI POSTA ELETTRONICA

L'AOO si dota di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento. Inoltre l'AOO si dota di caselle di posta elettronica - anche di tipo tradizionale – di appoggio ad ogni singolo ufficio, come da allegato 4.
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.

1.8 SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI: TITOLARIO

Con l'inizio della attività operativa del protocollo unico viene adottato un unico titolario di classificazione per l'archivio centrale unico dell'amministrazione, allegato 5 al presente Manuale.
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.
L'allegato 5 è suscettibile di modifica in caso di inserimento di nuovi "argomenti" o in caso di riorganizzazione dei medesimi. Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con RP e OP.

Dopo ogni modifica del Titolario, RSP provvede ad informare RP ed OP, dando loro le istruzioni per il corretto utilizzo delle classificazioni. Il Titolario non è retroattivo: non si applica cioè ai documenti protocollati prima della sua introduzione.
Di norma, le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo Titolario e valgono almeno per l'intero anno.
Il Titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'Amministrazione e approvato dai competenti organi.

1.9 DOCUMENTI DA PROTOCOLLARE E DOCUMENTI ESCLUSI

1.9.1 DOCUMENTI DA PROTOCOLLARE

Sono da protocollare i documenti ricevuti e spediti dalla AOO. Sono comunque oggetto di registrazione obbligatoria tutti i documenti dai quali possono nascere diritti, doveri o legittime aspettative di terzi.

1.9.2 DOCUMENTI DA NON PROTOCOLLARE

Alcune tipologie di documenti non devono essere protocollate, come da allegato 7. Tali documenti vanno conservati, ove se ne ravvisi l'opportunità, a cura dell'ufficio di competenza.

1.10 PIANO DI CONSERVAZIONE

Per la conservazione dei documenti, l'Ente si rifà alle normative specifiche vigenti.

1.11 FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le Amministrazioni dalla direttiva del Ministro della funzione pubblica sulla formazione e la valorizzazione del personale delle Pubbliche Amministrazioni, l'Amministrazione ha stabilito percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.
In particolare, considerato che il personale abilitato deve conoscere l'organizzazione, i compiti svolti da ciascun U 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, sono stati previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

- ai processi di semplificazione ed alle innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti della AOO;
- agli strumenti e alle tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione/AOO;
- alle norme sulla protezione dei dati personali e alle direttive impartite con il documento "Privacy, misure minime della sicurezza e adempimenti D.Lgs 196/2003".

TITOLO II
PIANO DI SICUREZZA

2.1 OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

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

2.2 GENERALITÀ

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

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso ai software gestionali;
- 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 D.Lgs. 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 annuale. 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 dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente dei software di gestione, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- gestione delle situazioni di emergenza informatica;
- 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;

- archiviazione giornaliera, in modo non modificabile, del registro di protocollo.

2.3 FORMAZIONE DEI DOCUMENTI E ASPETTI ATTINENTI ALLA SICUREZZA

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

- l'accesso esclusivamente tramite login e password del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.

Il sistema di gestione informatica dei documenti che più avanti verrà descritto in modo dettagliato :

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita e anche della PEC indicata o indicate dall'AOO;
- consente il reperimento delle informazioni riguardanti i documenti registrati e del registro di protocollo;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy";
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.3.1 COMPONENTE LOGICA DELLA SICUREZZA

La componente logica verificata ed attuata per la gestione del protocollo informatico, garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi:
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.
Risulta comunque ovvio che sono stati adottati i requisiti previsti dale buone regole di backup e disaster recovery e che vengono definite procedure sia semplici, come antivirus, etc, sia complesse, come sistemi di IPS e IDS.

2.4 CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI SOGGETTI A PROTOCOLLO

La conservazione dei documenti informatici segue le seguenti disposizioni :

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente dell'Agenzia
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

2.4.1 DESCRIZIONE DELLA SOLUZIONE

La soluzione effettua presso Aruba DocFly la conservazione dei Registri di protocollo informatico delle PA caricati sul documentale

L'utente carica sul Sistema documentale in cartelle organizzate in base alla PA i registri di protocollo con un file di segnatura e un file di log. Per ognuno di questi file carica un indice del pacchetto di versamento che ne contiene le informazioni utili alla creazione del pacchetto di archiviazione su Aruba Docfly.
Un task schedulato dal lunedì al venerdì raccoglie tutti gli indici caricati il giorno lavorativo precedente1 che non siano stati già conservati e li invia ad Aruba DocFly con tutti i documenti facenti parte del pacchetto di

versamento. DocFly, in caso non ci siano errori, genera il pacchetto di archiviazione non appena viene caricato l'ultimo file indicato negli indici.
Sul Sistema documentale l'indice e i documenti correlati vengono segnati come "conservati".

2.5 OPERAZIONI CLIENTE

2.5.1 RICHIESTA DI ATTIVAZIONE DI UNA NUOVA PA

Per attivare un account per una PA occorre fornire a Seen Solution tutti i dati indicati nell'appendice E più la scheda di conservazione allegata con dati e firma della PA.
In seguito Seen Solution comunicherà un nome utente e una password per accedere al Sistema documentale.

CARICAMENTO DEI REGISTRI

Le seguenti operazioni si intendono ripetute per ogni cartella delle PA.

- cerca la cartella con nome "Registro di Protocollo Informatico" all'interno della cartella root della PA
- effettua l'upload dei seguenti file
  - pdf di tipo "Registro_Giornaliero_di_Protocollo"
  - xml di tipo "Segnatura_di_Protocollo"
  - pdf di tipo "Log_di_Registro"
  - 3 xml di tipo "Indice_del_Pacchetto_di_Versamento" con nome che inizi con il prefisso "IPDV-" seguito da una stringa che renda univoco il nome all'interno del pacchetto di archiviazione.
- collega i file di segnatura e di log al registro
- collega ciascun indice al rispettivo documento

RICHIESTA DI STATO

Si può verificare se lo stato del workflow di un documento o dell'indice per capire a che punto del processo si trova. Gli stati sono tre:

- "Da versare su Aruba", il documento si trova in questo stato non appena viene caricato sul Sistema documentale
- "Versato su Aruba", il documento è stato caricato nell'archivio di DocFly ma non ha ancora passato le verifiche della piattaforma
- "Conservato nel Pacchetto di Archiviazione", il file è stato correttamente conservato sulla piattaforma aruba

Appendice A: Metodi del WS del Sistema documentale utilizzabili:

Ricerca della cartella "Registro di Protocollo Informatico"

Utilizzare la funzione get_folder_contents, in grassetto i parametri da variare:

```
...
   <soapenv:Body>
        <soapenv:get_folder_contents
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
        <session_id xsi:type="xsd:string">d9mq5qt6glidhb7ri55ldqo603</session_id>
        <folder_id xsi:type="xsd:int">890</folder_id>
        <depth xsi:type="xsd:int">1</depth>
        <what xsi:type="xsd:string">F</what>
        </soapenv:get_folder_contents>
   </soapenv:Body>
...
```

Dalla risposta selezionare il campo items->item->id della cartella con campo filename uguale a "Registro di Protocollo Informatico", i campi sono indicati in grassetto:

```
...
  <SOAP-ENV:Body>
      <SOAP-ENV:get_folder_contentsResponse>
      <item xsi:type="ns4:kt_folder_contents">
      <status_code xsi:type="xsd:int">0</status_code>
      <message xsi:type="xsd:string"/>
      <folder_id xsi:type="xsd:int">890</folder_id>
      <folder_name xsi:type="xsd:string">UF5Z7K</folder_name>
      <full_path xsi:type="xsd:string">Fepa_p test/UF5Z7K</full_path>
      <items xsi:type="SOAP-ENC:Array" SOAP- ENC:arrayType="ns4:kt_folder_item[2]"
  SOAP-ENC:offset="[0]">
      <item xsi:type="ns4:kt_folder_item">
      <id xsi:type="xsd:int">917</id>
      <item_type xsi:type="xsd:string">F</item_type>
      <custom_document_no xsi:type="xsd:string">n/a</custom_document_no>
      <oem_document_no xsi:type="xsd:string">n/a</oem_document_no>
      <title xsi:type="xsd:string">Registro di Protocollo
Informatico</title>
      <document_type xsi:type="xsd:string">n/a</document_type>
      <filename xsi:type="xsd:string">Registro di Protocollo
Informatico</filename>
          ...
      </item>
      <item xsi:type="ns4:kt_folder_item">
      <id xsi:type="xsd:int">918</id>
      <item_type xsi:type="xsd:string">F</item_type>
      <custom_document_no xsi:type="xsd:string">n/a</custom_document_no>
      <oem_document_no xsi:type="xsd:string">n/a</oem_document_no>
      <title xsi:type="xsd:string">Test</title>
      <document_type xsi:type="xsd:string">n/a</document_type>
      <filename xsi:type="xsd:string">Test</filename>
      ...
      </item>
  </items>
  </item>
  </SOAP-ENV:get_folder_contentsResponse>
</SOAP-ENV:Body>
  ...
```

Upload dei documenti

Le seguenti operazioni vanno ripetute per ognuno dei quattro tipi di documento indicati nel paragrafo "Operazioni".

Utilizzare la funzione get_document_type_metadata per recuperare le strutture dei metadati da compilare. Indicare nel campo document_type il tipo di documento:

```
...
   <soapenv:Body>
        <soapenv:get_document_type_metadata
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
        <session_id xsi:type="xsd:string">d9mq5qt6glidhb7ri55ldqo603</session_id>
        <document_type xsi:type="xsd:string">Registro_Giornaliero_di_Protocollo</docum
ent_type>
</soapenv:get_document_type_metadata>
   </soapenv:Body>
...
```

Riempire i campi metadata->fieldset->fields->field->value indicati in grassetto (ignorare il fieldset "Tag Cloud"):

```
...
   <SOAP-ENV:Body>
        <SOAP-ENV:get_document_type_metadataResponse>
        <return xsi:type="ns4:kt_metadata_response">
        <status_code xsi:type="xsd:int">0</status_code>
        <message xsi:type="xsd:string"/>
       <metadata xsi:type="SOAP-ENC:Array" SOAP-
ENC:arrayType="ns4:kt_metadata_fieldset[2]" SOAP-ENC:offset="[0]">
            <fieldset xsi:type="ns4:kt_metadata_fieldset">
            <fieldset xsi:type="xsd:string">Tag Cloud</fieldset>
            ...
            </fieldset>
            <fieldset xsi:type="ns4:kt_metadata_fieldset">
            <fieldset xsi:type="xsd:string">Registro di
Protocollo</fieldset>
            <description xsi:type="xsd:string">Registro di
Protocollo</description>
            <fields xsi:type="SOAP-ENC:Array" SOAP-
ENC:arrayType="ns4:kt_metadata_field[3]" SOAP-ENC:offset="[0]">
                <field xsi:type="ns4:kt_metadata_field">

                <name xsi:type="xsd:string">Codice Fiscale PA</name>
                <required xsi:type="xsd:boolean">false</required>
                <value xsi:type="xsd:string">n/a</value>
                <description xsi:type="xsd:string">Codice Fiscale PA</description>
                <control_type xsi:type="xsd:string">string</control_type>
                </field>
                <field xsi:type="ns4:kt_metadata_field">
                <name xsi:type="xsd:string">Data
Registro</name>
                <required
xsi:type="xsd:boolean">false</required>
                <value xsi:type="xsd:string">n/a</value>
                <description xsi:type="xsd:string">Data
Registro</description>
                <control_type
xsi:type="xsd:string">string</control_type>
                </field>
```

```
                                    <field xsi:type="ns4:kt_metadata_field">
                                        <name xsi:type="xsd:string">Numero di
                    Registro</name>
                                         <required
                    xsi:type="xsd:boolean">false</required>
                                        <value xsi:type="xsd:string">n/a</value>
                                        <description xsi:type="xsd:string">Numero di
                    Registro</description>
                                        <control_type
                    xsi:type="xsd:string">string</control_type>
                            </field>
                    </fields>
                    </fieldset>
                </metadata>
                </return>
                </SOAP-ENV:get_document_type_metadataResponse>
            </SOAP-ENV:Body>
        …
```

Caricare i documenti (codificati in base64) tramite *add_base64_document_with_metadata* inserendo i parametri in grassetto (utilizzare la struttura riempita precedentemente nel campo *metadata* e passare un'array vuoto nel campo *sysdata)*:

```
        …
            <soapenv:Body>
                <soapenv:add_base64_document_with_metadata
        soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
                <session_id xsi:type="xsd:string">d9mq5qt6glidhb7ri55ldqo603</session_id>
                <folder_id xsi:type="xsd:int">917</folder_id>
                <title xsi:type="xsd:string">20150929_azienda_a.pdf</title>
                <filename xsi:type="xsd:string">20150929_azienda_a.pdf</filename>
                <documentype xsi:type="xsd:string">Registro_Giornaliero_Di_Protocollo</docum
        entype>
                <base64 xsi:type="xsd:string">MjAxNTA5Mj...</base64>
                <metadata xsi:type="urn:kt_metadata_fieldsets"
        soapenc:arrayType="urn:kt_metadata_fieldset[]"
        xmlns:urn="urn:KnowledgeTree"/>
                <sysdata xsi:type="urn:kt_sysdata" soapenc:arrayType="urn:kt_sysdata_item[]"
        xmlns:urn="urn:KnowledgeTree"/>
</soapenv:add_base64_document_with_metadata>
            </soapenv:Body>
        </soapenv:Envelope>
```

Dalla risposta è possibile recuperare l'id del documento:

```
        …
            <SOAP-ENV:Body>
                <SOAP-ENV:add_base64_document_with_metadataResponse>
                <return xsi:type="ns4:kt_document_detail">
                <document_id xsi:type="xsd:int">194455</document_id>
```

<oem_document_no xsi:type="xsd:string">n/a</oem_document_no>
<title xsi:type="xsd:string">20150929_azienda_a.pdf</title>
<document_type xsi:type="xsd:string">Registro di Protocollo</document_type>
<filename xsi:type="xsd:string">20150929_azienda_a.pdf</filename>
<filesize xsi:type="xsd:int">7</filesize>
<folder_id xsi:type="xsd:int">917</folder_id>
<created_by xsi:type="xsd:string">Administrator</created_by>

…

Collegamento dei documenti

Utilizzare la funzione *link_documents* indicando gli id dei documenti da collegare:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema- instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header/>
   <soapenv:Body>
        <soapenv:link_documents
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
        <session_id xsi:type="xsd:string">d9mq5qt6glidhb7ri55ldqo603</session_id>
        <parent_document_id xsi:type="xsd:int">194455</parent_document_id>
        <child_document_id xsi:type="xsd:int">194456</child_document_id>
        <type xsi:type="xsd:string">Attachment</type>
        </soapenv:link_documents>
   </soapenv:Body>
</soapenv:Envelope>
```

Verifica dello stato di un documento

Per verificare lo stato di un documento occorre conoscerne l'id restituito al momento dell'upload. In alternativa è possibile recuperare la lista dei documenti utilizzando la funzione get_folder_contents illustrata all'inizio di questo paragrafo utilizzando il valore "D" per il parametro *what*

Utilizzare la funzione *get_document_detail*:

```
…
  <soapenv:Body>
        <soapenv:get_document_detail
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
        <session_id xsi:type="xsd:string">d9mq5qt6glidhb7ri55ldqo603</session_id>
        <document_id xsi:type="xsd:int">194455</document_id>
        <detail xsi:type="xsd:string"></detail>
        </soapenv:get_document_detail>
  </soapenv:Body>
</soapenv:Envelope>
```

Dalla risposta esaminare il campo workflow_state:

```
..
  <SOAP-ENV:Body>
        <SOAP-ENV:get_document_detailResponse>
        <return xsi:type="ns4:kt_document_detail">
              <document_id xsi:type="xsd:int">194455</document_id>
              <custom_document_no xsi:type="xsd:string">n/a</custom_document_no>
              <oem_document_no xsi:type="xsd:string">n/a</oem_document_no>
              <title xsi:type="xsd:string">20150929_azienda_a.pdf</title>
              <document_type
        xsi:type="xsd:string">Registro_Giornaliero_di_Protocollo</document
        _type>
              <filename xsi:type="xsd:string">20150929_azienda_a.pdf</filename>
              ...
              <workflow xsi:type="xsd:string">Conservazione
        RPI</workflow>
              <workflow_state xsi:type="xsd:string">Da versare ad
        Aruba</workflow_state>
              <full_path xsi:type="xsd:string">/Fepa_p test/UF5Z7K/Registro di
        Protocollo Informatico/20150929_azienda_a.pdf</full_path>
        </return>
        </SOAP-ENV:get_document_detailResponse>
  </SOAP-ENV:Body>
...
```

Appendice B: XML dell'indice

In allegato a questo documenti ci sono i template dei tre indici. Contengono lo stesso set di metadati e differiscono solo per il valore del tag <docClass>

Gli id che precedono i nomi delle classi vengono forniti da Seen Solution all'atto della creazione dell'utente PA in quanto vengono generati da Aruba Docfly in base all' archivio destinato alla PA. È possibile recuperare automaticamente questi indici leggendoli dal file "class_id.txt" presente nella cartella "Registro di Protocollo Informatico" della PA, che avrà ad esempio questa forma:

```
Registro_Giornaliero_di_Protocollo=1440
Segnatura_di_Protocollo=1441
Log_di_Registro=1442
```

All'interno dell'indice per ciascun documento sono obbligatori imetadati:

- <docid> - assegna al documento un identificativo univoco, dal lato di chi versa, al singolo documento. Normalmente tale dato viene ottenuto da un sistema documentale
- <filename> - indica il nome del documento, comprensivo di eventuale estensione, così come viene memorizzato su file system
- <mimetype> - indica il tipo di documento, nel senso informatico del termine, secondo la RFC 2046
- <closingDate> - indica la data di chiusura del documento, ovvero la data di ultima modifica precedente alla messa in conservazione
- <hash> - contiene l'impronta del documento prodotte esclusivamente tramite SHA-256 e codificate in base64

I metadati nella sezione <mandatory> devono essere presenti nell'indice ma è obbligatorio valorizzare solo i campi singlemetadata->value che hanno i nomi indicati di seguito, gli altri possono essere lasciati vuoti:

- <complexmetadata> "soggettoproduttore"
- se presente un secondo produttore:
    - Nome_soggetto_produttore_2
    - Cognome_soggetto_produttore_2
    - Codice_fiscale_soggetto_produttore_2
- Codice_identificativo_amministrazione_(IPA)
- Denominazione_dellamministrazione
- aooDiRiferimento
- per il responsabile della gestione documentale:
    - Cognome_responsabile_gestione_documentale
    - Nome_responsabile_gestione_documentale
    - Codice_fiscale_responsabile_gestione_documentale
- oggettodocumento
- Codice_identificativo_del_registro
- Numero_progressivo_del_registro
- Anno
- Numero_prima_registrazione_effettuata_sul_registro
- Numero_ultima_registrazione_effettuata_sul_registro
- Data_prima_registrazione_effettuata_sul_registro
- Data_ultima_registrazione_effettuata_sul_registro

I metadati nella sezione <extraInfos> possono non figurare nell'indice.

Appendice C: XML della segnatura

Di seguito sono indicati i dati da inserire nel file xml della segnatura:

- Codice indentificativo PA
- Codice indentificativo Area Organizzativa Omogenea

Per ogni protocollo:

- Data di protocollo
- Progressivo di protocollo
- Oggetto protocollo
- Mittente
- Destinatario
- Impronta SHA256
- Allegati (con impronta SHA256)

Appendice D: Tipi e metadati definiti nel Sistema documentale

Ai seguenti tre tipi

- "Registro_Giornaliero_di_Protocollo"
- "Segnatura_di_Protocollo"

- "Log_di_Registro"

è associato il seguente set di metadati che corrispondono a quelli indicati come obbligatori per gli indici nell'appendice B:

- docid
- closingDate
- hash
- soggettoproduttore_cognome
- soggettoproduttore_denominazione
- soggettoproduttore_codicefiscale
- soggettoproduttore_partitaiva
- soggettoproduttore_nome
- Nome_soggetto_produttore_2
- Cognome_soggetto_produttore_2
- Codice_fiscale_soggetto_produttore_2
- Codice_identificativo_amministrazione_(IPA)
- Denominazione_dellamministrazione
- aooDiRiferimento
- Cognome_responsabile_gestione_documentale
- Nome_responsabile_gestione_documentale
- Codice_fiscale_responsabile_gestione_documentale
- oggettodocumento
- Codice_identificativo_del_registro
- Numero_progressivo_del_registro
- Anno
- Numero_prima_registrazione_effettuata_sul_registro
- Numero_ultima_registrazione_effettuata_sul_registro
- Data_prima_registrazione_effettuata_sul_registro
- Data_ultima_registrazione_effettuata_sul_registro

Al tipo "Indice_del_Pacchetto_di_Versamento" sono associati i metadati

- pdvid
- Data
- Classe_documentale
- Codice_ufficio_pa
- Codice_fiscal_pa
- Partita_iva_pa

Appendice E: Dati anagrafici per attivazione PA

Vengono di seguito elencati i dati richiesti per l'attivazione di un nuovo archivio per la PA:

Dati fiscali PA	Referente archivio
• Ragione sociale • Partita IVA • Codice Fiscale • Codice ufficio • Indirizzo • CAP • Comune • Provincia • Stato	1. Nome 2. Cognome 3. Codice fiscale 4. Telefono 5. Email 6. Pec 7. Sesso 8. Data di nascita 9. Comune di nascita 10. Provincia di nascita 11. Stato di nascita 12. Indirizzo di residenza 13. CAP di residenza 14. Comune di residenza 15. Provincia di residenza 16. Stato di residenza

2.6 ASPETTI DI SICUREZZA

Per tutti gli aspetti di sicurezza non specificatamente trattati nel presente manuale, si fa riferimento al documento "Privacy, misure minime della sicurezza e adempimenti D.Lgs 196/2003".

2.7 ACCESSO AL REGISTRO DI PROTOCOLLO

L'accesso al Registro di protocollo è consentita al personale dipendente con le abilitazioni previste (allegato 2).

TITOLO III
PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

3.1 UNICITA' DEL PROTOCOLLO INFORMATICO

Il Registro di Protocollo è unico e la registrazione è progressiva.
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.
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 protocollata viene considerata giuridicamente inesistente presso l'Amministrazione.
Non è consentita la protocollazione di un documento già protocollato.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

3.2 REGISTRO GIORNALIERO DI PROTOCOLLO

Il RSP, o suo delegato, 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 viene generato, al termine della giornata lavorativa, dal RP ed inviato al RC, appositamente nominato, che provvederà alla sua archiviazione.

3.3 REGISTRAZIONE DI PROTOCOLLO

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

Il registro giornaliero di protocollo deve ricomprendere le informazioni minime richieste dall'art. 53, co. 1, del DPR 445/2000 e dalla Circolare n. 60 del 201311. In particolare, la registrazione di protocollo per ogni documento ricevuto o spedito richiede la memorizzazione delle seguenti informazioni:

- il numero di protocollo del documento generato automaticamente dal sistema;
- la data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
- l'oggetto del documento;
- la data e il protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica;
- indicazione del registro nell'ambito del quale è stata effettuata la registrazione.

Di conseguenza, il registro giornaliero di protocollo deve contenere, in modo ordinato e progressivo, l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Le regole sulla formazione dei registri e repertori informatici sono contenute nell'art. 14 del DPCM 13 novembre 201412. In particolare, il primo comma dell'articolo richiamato stabilisce che il registro di protocollo13 è formato ai sensi dell'art. 3, comma 1, lettera d), 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".

Nella fase di formazione del registro giornaliero di protocollo quindi, deve essere, in primis, garantita la staticità del documento informatico contenente le registrazioni effettuate nell'arco dello stesso giorno. Secondo quanto disposto dalle regole tecniche14, la staticità di un documento informatico è rappresentata dalla capacità dello stesso di garantire "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". Garantita la staticità del documento informatico "Registro giornaliero di protocollo", è necessario garantire anche la sua immodificabilità15 e integrità16 nel tempo. L'art. 3, del DPCM 13.11.2014, al co. 6, stabilisce che nel caso di documento informatico formato ai sensi del comma 1, lettera d), come nel caso di specie, le caratteristiche di immodificabilità e di integrità sono determinate con la produzione di un'estrazione statica dei dati e il trasferimento della stessa nel Sistema di Conservazione. Il documento informatico "Registro giornaliero di protocollo" dovrà quindi possedere le seguenti tre caratteristiche: - staticità; - immodificabilità; - integrità

La scelta dei formati idonei alla conservazione del Registro giornaliero di protocollo deve, quindi, essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità sopra richiamate. E' pertanto opportuno fare riferimento all'allegato 2, "Formati", delle regole tecniche.

I metadati sono un insieme di dati (ergo, informazioni) associati a un documento informatico utili per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel Sistema di Conservazione. Nell'allegato 5 alle regole tecniche in commento, sono riportati i metadati minimi da associare ad ogni documento informatico ai quali, nel caso di specie, è opportuno aggiungerne degli ulteriori.

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.

3.3.1. DOCUMENTI INFORMATICI

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

3.3.2. DOCUMENTI ANALOGICI (CARTACEI E SUPPORTI RIMOVIBILI)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).
La registrazione di protocollo di un documento analogico cartaceo ricevuto viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

3.4 ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO

Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- ora e minuto di registrazione;
- i riferimenti del documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- collegamento a documenti precedenti e susseguenti;
- nominativo dei destinatari delle copie per conoscenza;

3.5 SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo (numero progressivo, data di protocollo, e ufficio competente).
Essa consente di individuare ciascun documento in modo inequivocabile.

3.6 MODIFICA O ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

I protocolli inseriti da un determinato utente NON possono essere modificati da altri utenti (ad esclusione del Responsabile di Gestione).

Dopo l'avvenuto invio nel sistema di conservazione (giorno lavorativo successivo), NON è più possibile apportare modifiche ai protocolli neppure da colui il quale li ha inseriti/registrati. L'unica operazione ammessa è l'ANNULLAMENTO da parte del Responsabile di Gestione.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

3.7 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

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

3.7.1.TELEGRAMMI

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

3.7.2 TELEFAX

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

Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.
L'accertamento della fonte di provenienza spetta al RP e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.
Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RP provvede ad acquisire l'originale.
La segnatura viene apposta sul documento e non sulla copertina di trasmissione.
La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

3.7.3 DOMANDE DI PARTECIPAZIONE A CONCORSI E/O SELEZIONI, AVVISI, CORSI

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

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

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

3.7.5 PROTOCOLLI URGENTI

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

3.7.6 DOCUMENTI NON FIRMATI

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

3.7.7 PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

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

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

3.7.8 PROTOCOLLO DI DOCUMENTI PERVENUTI ERRONEAMENTE

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

3.7.9 DIFFERIMENTO DELLE REGISTRAZIONI

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 24 ore lavorative dal ricevimento di detti documenti.
Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previa autorizzazione del RSP.

3.7.10 CORRISPONDENZA PERSONALE O RISERVATA

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

3.7.11 INTEGRAZIONI DOCUMENTARIE

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

3.8 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL SOFTWARE DEDICATO

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

3.9 REGISTRAZIONI DI PROTOCOLLO

3.9.1 ATTRIBUZIONE DEL PROTOCOLLO

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

3.9.2 REGISTRO INFORMATICO DI PROTOCOLLO

Il sistema di *protocollo informatico* assicura:

- **univoca identificazione** ed autentificazione degli utenti
- la **protezione delle informazioni** relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli **utenti abilitati**;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da **garantirne l'identificazione**.

Il sistema di protocollo informatico deve consentire il **controllo differenziato dell'accesso** alle risorse del sistema per ciascun utente o gruppo di utenti nonché il **tracciamento di qualsiasi evento di modifica** delle informazioni trattate e l'individuazione del suo autore.
Il registro giornaliero di protocollo è **trasmesso** entro la giornata lavorativa successiva al sistema di conservazione, garantendone **l'immodificabilità del contenuto**.
È inoltre disponibile, all'occorrenza, una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

3.9.3 FILE

Tutti i files allegati vengono salvati all'interno di un database specifico creatosi in automatico;nel sistema di conservazione digitale vengono inviate esclusivamente le impronte digitali dei documenti allegati (sha256-hash) e non i fisici documenti.

3.9.4 LOG

Ogni protocollo ha la sua videata di log in cui vengono memorizzate tutte le operazioni effettuate sul protocollo stesso indicando data/ora/utente/tipo di operazione (inserimento / modifica / annullamento / archiviazione).

3.9.5 ARCHIVIAZIONE/CONSERVAZIONE

Il sistema genera i files che vengono inviati in automatico in archiviazione sostituiva.

Automaticamente, il giorno successivo alle ore 12.00, il programma genera ed invia al sistema di conservazione i seguenti files:

- File PROTOCOLLO.pdf/A del giorno richiesto con Impronta sha256 del protocollo ed eventuali file allegati *(NON VENGONO ARCHIVIATI I FILES MA SOLO L'IMPRONTA SHA256-HASH DEGLI STESSI)*.
- File LOG.pdf/A del giorno richiesto: riporta le informazioni dei protocolli ed eventuali allegati in formato XML.
- 3. File METADATI.xlm del giorno richiesto : riassume brevemente il contenuto dei documenti in modo da facilitarne l'identificazione.

3.9.6 TERMINOLOGIA

- **Formato di stampa PDF/A:** Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali.
  Tra le caratteristiche di questa tipologia di file abbiamo:
  - assenza di collegamenti esterni;
  - assenza di codici eseguibili quali javascript ecc…;
  - Assenza di contenuti crittografati.

- **SHA256 – HASH**-: codice fiscale univoco del protocollo e degli eventuali allegati. E' una funzione matematica che genera, a partire da una evidenza informatica, una impronta unica in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali.

3.10 RILASCIO DELLE ABILITAZIONI DI ACCESSO

Il controllo degli accessi è il processo che garantisce la gestione del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.
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);
  - 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, come da allegato 2, che si avvale di un utente così detto privilegiato (amministratore).
Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli OP abilitati allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono riportate nell'allegato 2 e sono costantemente aggiornate a cura del RSP.

3.10.1 ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO

Gli utenti abilitati accedono al software "protocollo informatico" fornito da CBA Group utilizzando il proprio userID e la propria password.
Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.

3.11 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

3.11.1 IL REGISTRO DI EMERGENZA

Qualora non fosse disponibile fruire del software per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza come da allegato 6.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.
Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RSP annota sullo stesso il mancato uso.
Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale.
Il registro di emergenza si configura come un repertorio del protocollo generale.
Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.
A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.
I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.
La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.
In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo

3.11.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

Il RSP assicura che, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica, le operazioni di protocollo siano svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea.
Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.
Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.
Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RSP ha predisposto il modulo riportato nell'allegato 6.
L'elenco delle persone abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 2.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il RSP autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

3.11.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

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

3.11.4 MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA

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

È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.
Una volta ripristinata la piena funzionalità del protocollo, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.
Per semplificare la procedura di chiusura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) analogo a quello utilizzato nella fase di apertura del registro di emergenza.

TITOLO IV
NORME TRANSITORIE E FINALI

4.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

L'amministrazione adotta il presente "Manuale di gestione" su proposta del RSP.
Il presente Manuale potrà essere aggiornato a seguito di:

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

4.2 PUBBLICITÀ DEL PRESENTE MANUALE

Il presente Manuale, ai sensi del DPCM 3 dicembre 2013, è reso disponibile alla consultazione del pubblico tramite pubblicazione sul sito istituzionale.

4.3 OPERATIVITÀ DEL PRESENTE MANUALE

Il presente regolamento è operativo dal 12 ottobre 2015 come previsto dal DPCM 3 dicembre 2013.

Allegati:

1. Uffici che compongono la AOO e individuazione responsabile
2. Mappa dei ruoli e delle abilitazioni
3. Elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione
4. Elenco mail aziendali
5. Titolare e piano di conservazione e di scarto
6. Modello registro di emergenza
7. Elenco documenti esclusi dalla registrazione di protocollo
8. Diagramma del flusso documentale