# MANUALE DI GESTIONE DOCUMENTALE

## Art. 5 DPCM 3.12.2013

***Versione 1.0***

*A.P.S.P. U. Campagnola*
*Via Campagnola, 5*
*38063 – Avio (TN)*

Adottato dal Consiglio di Amministrazione con Deliberazione n. 4 del 22 gennaio 2016.

# SOMMARIO

1. PRINCIPI GENERALI ..... 3
1.1 Premessa ..... 3
1.2 Definizioni e norme di riferimento ..... 3
1.3 Area Organizzativa Omogenea ..... 4
1.4 Servizio per la gestione informatica del protocollo ..... 4
1.5 Tutela dei dati personali ..... 5
1.6 Caselle di Posta Elettronica ..... 5
1.7 Accreditamento dell'AOO all' IPA ..... 5
2. PIANO DI SICUREZZA PER LA GESTIONE DEI DOCUMENTI INFORMATICI ..... 6
2.1 Obiettivi del piano di sicurezza ..... 6
2.2 Generalità ..... 6
2.3 Formazione dei documenti – Aspetti attinenti alla sicurezza ..... 7
2.3.1 Componente logica della sicurezza ..... 7
2.3.2 Componente infrastrutturale della sicurezza ..... 8
3. CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI SOGGETTI A PROTOCOLLO ..... 9
3.1 Descrizione della soluzione ..... 9
3.2 Operazioni cliente ..... 9
3.2.1 Richiesta di attivazione di una nuova PA ..... 9
3.2.2 Caricamento dei registri ..... 9
3.2.3 Richiesta di stato ..... 10
4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI 11
4.1 Documento ricevuto ..... 11
4.2 Documento inviato ..... 12
4.3 Documento interno ..... 12
4.4 Formazione del registro di protocollo e dei documento soggetti a protocollazione ..... 12
4.5 Posta elettronica certificata ..... 13
5. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE ..... 15
5.1 Documenti esclusi ..... 15
5.2 Documenti soggetti a registrazione particolare ..... 15

6. SISTEMA SOFTWARE DI CLASSIFICAZIONE, FASCICOLAZIONE E DI PROTOCOLLO INFORMATICO ..... 16
6.1 Ricerca protocolli ..... 16
6.2 Raggruppamento esibenti/argomenti ..... 16
6.3 Gestione multipla inserimento protocolli ..... 17
6.4 Protocollo informatico pubblica amministrazione ..... 17
6.5 Creazione/modifica password d'accesso ..... 17
6.6 Area organizzativa omogenea (aoo) – Enti interni ..... 18
6.7 Disposizioni riferite al sistema software adottato ..... 18
6.8 Creazione/invio files ..... 19
7 DISPOSIZIONI FINALI ..... 20
7.1 Modalità di approvazione e aggiornamento del manuale ..... 20
7.2 Disposizioni abrogate ..... 20
7.3 Pubblicità del presente Manuale ..... 20
7.4 Operatività del presente manuale ..... 20
Appendice A: Metodi del WS del Sistema documentale utilizzabili ..... 21
Appendice B: XML dell'indice ..... 27
Appendice C: XML della segnatura ..... 29
Appendice D: Tipi e metadati definiti nel Sistema documentale ..... 30
Appendice E: Dati anagrafici per attivazione PA ..... 31

# 1. PRINCIPI GENERALI

## 1.1 Premessa

II decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", articolo 3, comma 1, lettera d), prevede l'adozione del manuale di gestione per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale, dal successivo art. 5, comma 1, "descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".
Dunque ogni pubblica amministrazione deve individuare 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'articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000).
Si precisa che con deliberazione n. 11 del 9 novembre 2015 il Consiglio di Amministrazione, vista la struttura organizzativa dell'Azienda, ha individuato un'unica Area Organizzativa Omogena.
Il seguente Manuale di gestione descrive in dettaglio sia il sistema di gestione documentale, sia le funzionalità del protocollo informatico, secondo quanto dettato dal DPCM del 3 Dicembre 2013.
Il presente documento, pertanto, si rivolge sia agli utenti autorizzati alla gestione del protocollo, compreso ovviamente il responsabile della gestione documentale, sia a tutti i dipendenti della PA ed è stato redatto ai sensi dell'articolo 3, comma 1, lettera d) del decreto del Presidente del Consiglio del 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", descrivendone anche le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi della PA.
Si precisa che l'A.P.S.P. nel mese di ottobre 2015 ha provveduto a sottoscrivere, con la Società CBA Informatica Srl, un contratto di fornitura dei servizi per la gestione in outsourcing del processo di conservazione a norma di qualunque tipologia di documento informatico secondo quanto previsto dalle normative vigenti in materia. Il contratto prevede altresì che il servizio di cui sopra nonché quelli consulenziali, tecnico-normativi, sulle tematiche della conservazione sostitutiva, protocollo informatico, gestione elettronica documentale e codice dell'Amministrazione Digitale, sia gestito dalla Società Seen Solution Srl.

## 1.2 Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

- "Amministrazione" o "Azienda", l'A.P.S.P. U. Campagnola di Avio;
- "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;
- "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico";
- "Codice", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.

Per le definizioni vedasi l'elenco riportato nell'allegato 1.
Di seguito si riportano gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea;
- MG - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- RPI - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;

Comunque sia, in questo manuale verranno utilizzati altri termini, che saranno spiegati man mano nell'argomentazione successiva.

### 1.3 Area Organizzativa Omogenea

Per la gestione dei documenti l'Azienda ha istituito un'unica Area Organizzativa Omogenea (AOO) dove è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
All'interno dell'amministrazione il sistema archivistico è unico.
All'interno della AOO il sistema di protocollazione è totalmente centralizzato, nel senso che tutta la corrispondenza, in ingresso e in uscita, è gestita da più utenti ma da una sola Area.

### 1.4 Servizio per la gestione informatica del protocollo

Nell'AOO è presente il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il responsabile del servizio di protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RPI), nominato con provvedimento del Consiglio di Amministrazione ed individuato nella figura del Direttore. Il Consiglio di Amministrazione ha altresì provveduto alla nomica di un vicario.
In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, 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 istituzionale dell'amministrazione ai sensi dell'amministrazione trasparente;
- abilitare gli utenti dell'AOO all'utilizzo del protocollo;
- garantire il rispetto della normativa durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta conservazione giornaliera del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento dei software interni all'AOO e il rispetto delle procedure atte a garantire la 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 eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili;

- garantire che il documento protocollo informatico sia integro, qualitativamente corretto, immodificabile e visualizzabile.

### 1.5 Tutela dei dati personali

L'A.P.S.P., titolare dei dati di protocollo e dei dati personali, comuni, sensibili e/o giudiziari, contenuti nella documentazione amministrativa di propria competenza, ha ottemperato al dettato del decreto legislativo 30 giugno 2003, n.196 con atti formali aventi rilevanza interna ed esterna.

### 1.6 Caselle di Posta Elettronica

L'AOO è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita (apspavio@pec.it)

### 1.7 Accreditamento dell'AOO all' IPA

L'AOO si è dotata di una casella di posta elettronica certificata attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, e sulla quale si garantisce la lettura almeno una volta al giorno. La corrispondenza ricevuta i sabati ed i giorni festivi sarà visualizzata il primo giorno feriale successivo.
Il codice identificativo della PA è stato generato e attribuito autonomamente dall'amministrazione. L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.
L'accreditamento all'IPA, peraltro già avvenuto per la Fattura Elettronica verso la Pubblica Amministrazione, ha permesso alla presente A.P.S.P. di avere il codice di riferimento che verrà gestito ed inserito nel registro di protocollo, sottoposto a conservazione. Il codice IPA attribuito all'A.P.S.P. è il seguente: "auc".

# 2. PIANO DI SICUREZZA PER LA GESTIONE DEI DOCUMENTI INFORMATICI

## 2.1 Obiettivi del piano di sicurezza

Il presente capitolo, ai sendi dell'art. 5, comma 2 lettera b) del DPCM 3/12/2013, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.
Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla 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

L'RPI ha definito, d'intesa con i collaboratori del servizio interno "Comunicazione, Trasparenza e privacy" dell'Azienda, le misure di di sicurezza per la gestione del protocollo informatico.Tali misure sono state identificate mediante 'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati, e sulla base delle disposizioni stabilite dal vertice dell'amministrazione. Il piano di sicurezza difinisce quanto segue:

- le politiche generali e particolari di sicurezza adotatte all'interno della AOO;
- le modalità di accesso ai software gestionali ed al servizio protocollo, di gestione documentale e archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del 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 biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
L'RPI 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:

- 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 o semestrale in base alla natura dei dati trattati;

- 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;
- verifica del corretto funzionamento dei sistemi informativi;
- 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 – 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 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.
Sono altresì stati adottati i requisiti previsti in materia di backup e disaster recovery e procedure sia semplici, come antivirus, etc, sia complesse, come sistemi di IPS e IDS.

### 2.3.2 Componente infrastrutturale della sicurezza

Presso la PA, sono presenti i seguentiimpianti:

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

# 3. 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.

## 3.1 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 precedente[1] 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".

## 3.2 Operazioni cliente[2]

### 3.2.1 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.

### 3.2.2 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 file3
    - pdf di tipo "Registro_Giornaliero_di_Protocollo"

[1] Il lunedì processa i documenti caricati venerdì, sabato e domenica
[2] la lista dei metodi del ws che il cliente dovrà utilizzare si trova nell'appendice A
[3] il set di metadati per Ktreedoc è indicato nell'appendice D

- xml di tipo "Segnatura_di_Protocollo"[4]
- pdf di tipo "Log_di_Registro"
- 3 xml di tipo "Indice_del_Pacchetto_di_Versamento"[5] 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.

### 3.2.3 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

[4] i dati da inserire nel file di segnatura sono indicati nell'appendice C
[5] informazioni più dettagliate sugli indici si trovano nell'appendice B

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

II presente paragrafo spiega in modo sufficiente ma esausitivo il modo in cui i documenti vengono gestiti dall'A.P.S.P..
Nell'ambito del processo di gestione documentale, il documento amministrativo è così classificabile:

- ricevuto;
- inviato;
- interno.

Il documento amministrativo è così classificabile:

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "*1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*" e "*2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità*".
Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, che avverà l'11 Agosto 2016, il documento amministrativo può essere disponibile anche nella forma analogica e quindi non digitale/elettronica.

### 4.1 Documento ricevuto

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

- a mezzo posta elettronica convenzionale
- a mezzo posta elettronica certificata;
- su supporto rimovibile quale, ad esempio, cd rom, dvd, floppy disk, tape, pen drive.

Un documento analogico può essere, invece, recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telegramma;
- a mezzo fax;
- consegna a mano.

Tutti i documenti arrivati, mediante uno qualunque dei mezzi citati sono fatti pervenire, a cura del personale che li riceve, all'Ufficio di Protocollo.
I documenti ricevuti dall'A.P.S.P., se rientranti tra i documenti per i quali vi è l'obbligo di protocollo, vengono protocollati nel registro dell'A.P.S.P. Sui documenti non soggetti all'obbligo di cui sopra viene comunque apposto il timbro recante la data di ricezione degli stessi e la sigla di classificazione ai fini della relativa archiviazione.
In tale fase di avvio del processo di digitalizzazione della documentazione i soli documenti informatici ricevuti vengono allegati al sistema di gestione del protocollo informatico.

Tutti i documenti, compresi quelli informatici, vengono archiviati sulla base del titolario di classificazione adottato da parte dell'A.P.S.P..

### 4.2 Documento inviato

I documenti da spedire su supporto cartaceo vengono inviati al destinatario solo dopo che sono state eseguite le operazioni di registrazione di protocollo, segnatura di protocollo.
La spedizione di un documento informatico avviene via posta elettronica. Il documento informatico dopo essere stato protocollato viene, se previsto nel procedimento, firmato digitalmente e spedito all'indirizzo di posta elettronica del destinatario. L'A.P.S.P. utilizza a tal proposito anche la posta elettronica certificata.

### 4.3 Documento interno

I documenti interni si distinguono in documenti di prevalente carattere informativo e documenti aventi rilevanza giuridica. I primi sono, di norma, memorie informali, appunti, brevi comunicazioni, documenti informali che consentono la gestione e l'organizzazione interna. Tali documenti non devono essere registrati. I secondi sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti l'attività svolta o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Tali documenti devono essere registrati.

### 4.4 Formazione del registro di protocollo e dei documento soggetti a protocollazione

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 Agid n. 60 del 2013. In particolare, la registrazione di protocollo per ogni documento ricevuto o spedito richiede la memorizzazione delle seguenti informazioni:

a. il numero di protocollo del documento generato automaticamente dal sistema;
b. la data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c. il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
d. l'oggetto del documento;
e. la data e il protocollo del documento ricevuto, se disponibili;
f. l'impronta del documento informatico, se trasmesso per via telematica;
g. 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 2014. In particolare, il primo comma dell'articolo richiamato stabilisce che il registro di protocollo 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 tecniche, 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 immodificabilità e integrità nel tempo. L'art. 3, del DPCM 13.11.2014, al comma 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. È 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.

### 4.5 Posta elettronica certificata

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

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

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

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

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

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

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

# 5. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

## 5.1 Documenti esclusi

Sono, esclusi dalla registrazione di protocollo tutti i seguenti documenti:

- le gazzette ufficiali;
- i bollettini ufficiali e notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste, i libri, i materiali pubblicitari;
- gli inviti a manifestazioni;
- tutti i documenti non sottoscritti;
- presentazione di eventi formativi e/o seminari;
- convocazioni a corsi di formazione e/o aggiornamento;
- atti di mera gestione interna del personale (quali a titolo di esempio: richiesta ferie o recupero ore, autocertificazione per giustificare assenze, medello missione, autorizzazione al lavoro straordinario, variazione/aggiornamento dati anagrafici, certificati di malattia…);
- i documenti erroneamente indirizzati all'Azienda;
- le circolari che non contengono una interpretazione della normativa di riferimento;
- la corrispondenza interna ed esterna esclusa quella che in modo diretto o indiretto ha contenuto probatorio e comunque attiene alla gestione dei procedimenti amministrativi.

## 5.2 Documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti di seguito riportati:

- Deliberazioni del Consiglio di Amministrazione, Decreti del Presidente, Determinazioni del Direttore i quali non sono soggetti alla registrazione di protocollo ma riportano la numerazione progressiva;
- i documenti pubblicati all'albo on line dell'A.P.S.P. riportano il numero progressivo di repertorio. Alcuni documenti, considerata la loro rilevanza, potrebbero essere anche oggetto di registrazione nel protocollo;
- tutti i documenti contabili ad evidenza fiscale costituenti il ciclo attivo per i quali il documento viene emesso con numerazione progressiva;
- tutti i documenti contabili ad evidenza fiscale costituenti il ciclo passivo per i quali vi è l'obbligo di utilizzo della trasmissione in formato elettronico del documento e per i quali devono essere seguite le indicazioni previste dal D.L. 66/2014.

# 6. SISTEMA SOFTWARE DI CLASSIFICAZIONE, FASCICOLAZIONE E DI PROTOCOLLO INFORMATICO

Di seguito viene descritta la soluzione per il protocollo informatico, comprensiva di fascicolazione e di classificazione dei documenti oggetto di protocollo ed è utile anche all'utente autorizzato alla protocollazione e alla fascicolazione e classificazione della pratica.
La schermata che appare aprendo il programma è quella di registrazione dei protocolli; questa scelta operativa evita qualche passaggio inutile in quanto le operazioni che vengono svolte solitamente nel programma sono quelle di registrazione e/o di ricerca. Premendo quindi il pulsante NUOVO si da iniizo alla registrazione; nella registrazione vengono proposte ANNO, DATA e NUMERO PROTOCOLLO (quest'ultimo solitamente è il numero progressivo dell'anno ed è conforme a quanto dettato dalla normativa). Per ogni nuova registrazione viene ovviamente identificato il TIPO, l'ARGOMENTO dove sono collegati i riferimenti di archivio e l'OGGETTO del protocollo. Il protocollo inoltre viene gestito con la possibilità di modificare i riferimenti di archivio.
Inoltre nella scelta del Mittente e/o del Destinatario è possibile avere :

- ESIBENTE: attinge dalla tabella Esibenti specifica del programma Protocollo.
- CLIENTE/FORNITORE: attinge dalle anagrafiche clienti/fornitore della Contabilità Economica/Finanziaria.
- OSPITI: attinge dal fascicolo ospiti della Contabilità Ospiti / Contabilità Utenti / CSS.
- PERSONE DI RIFERIMENTO: attinge dalle persone di riferimento della Contabilità Ospiti Contabilità Utenti / CSS.
- DIPENDENTI:attingedall'anagraficadei dipendenti del software Stipendi/Presenze/Turni.

È inoltre possibile gestire sia le SPESE sia la TIPOLOGIA DI SPEDIZIONE, sia gli uffici di competenza del documento protocollato.

## 6.1 Ricerca protocolli

I parametri di ricerca dei protocolli registrati sono:

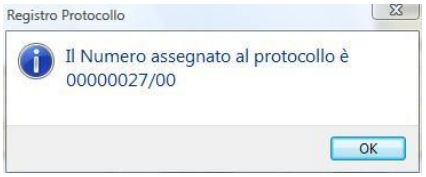
- dalla data movimento … alla data movimento…
- dal numero protocollo … al numero protocollo …
- tipologia di protocollo
- dalla data alla data di riferimento per i protocolli in arrivo
- numero di riferimento per i protocolli in arrivo
- stato protocollo (tutti – stampati – annullati)
- mittente/i – destinatario/i – tutti
- argomento/i – tutti
- ufficio/i – tutti
- parola nell'oggetto

## 6.2 Raggruppamento esibenti/argomenti

La funzione consente di raggruppare Esibenti e/o Argomenti per una razionalizzazione dei dati gestiti nel corso degli anni.
È possibile scegliere l'operazione '**RAGGRUPPA ESIBENTI**' per ottenere l'elenco dei mittenti/destinatari, selezionare tramite flag le anagrafiche da raggruppare, selezionare il tipo di esibente e l'anagrafica desiderata ed infine premere il pulsante ELABORA. La nuova anagrafica sostituirà l'informazione nei protocolli già registrati e stampati di tutti gli anni.
Procedura analoga anche con l'opzione '**RAGGRUPPA ARGOMENTI**'; selezionare gli argomenti che si desiderano raggruppare e successivamente l'argomento che sostituirà nei protocolli già registrati quelli selezionati. In questo modo l'argomento prescelto sostituirà quelli selezionati in tutti i protocolli già registrati.

### 6.3 Gestione multipla inserimento protocolli

Il sistema consente l'inserimento multiplo contemporaneo dei dati nel registro protocollo. In automatico sarà il programma ad assegnare il numero di protocollo corretto nell'eventualità di registrazione multipla dei protocolli da parte di più operatori. L'operatore che si troverà in questa situazione sarà avvertito da un messaggio simile a quello riportato di seguito.




Il messaggio testimonia che il numero di protocollo assegnato in precedenza nella fase iniziale di registrazione è stato assegnato all'utente che per primo ha terminato e confermato l'operazione di inserimento; in questo caso al secondo utente, dopo aver confermato il suo inserimento, apparirà il messaggio.

### 6.4 Protocollo informatico pubblica amministrazione

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.
Il sistema di protocollo informatico deve consentire 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**.

### 6.5 Creazione/modifica password d'accesso

Gli utenti che hanno accesso al software PROTOCOLLO INFORMATICO devono essere obbligatoriamente inseriti all'interno del sistema Password che identificherà gli utenti corrispondenti a persone fisiche (nome e cognome) e NON ad esempio utenti tipo UFFICIO PROTOCOLLO o UFFICIO AMM.VO.

Tra gli utenti abilitati all'accesso nel Protocollo è identificato il **Responsabile di Gestione** (responsabile o dirigente interno alla Struttura) il quale potrà:

- ANNULLARE i protocolli registrati dai colleghi/collaboratori (tale informazione sarà registrata nel file LOG ed inviata in archiviazione digitale);
- MODIFICARE i protocolli registrati dai colleghi/collaboratori se NON ancora inviati in archiviazione digitale (tale informazione sarà registrata nel file LOG ed inviata in archiviazione digitale).

### 6.6 Area organizzativa omogenea (aoo) – Enti interni

Il registro protocollo deve far riferimento all'Area Organizzativa Omogena (AOO) dell'Ente.
Nel caso in cui vi siano più AOO, ogn'una di esse dovrà avere una numerazione separata progressiva del proprio registro di protocollo.
Per adempiere a questa indicazione, il sistema si avvale della funzione 'Enti protocollo/A.O.O.'
Possono presentarsi due situazioni:

1. Nel caso in cui non sia mai stata abilitata tale funzione, in automatico verrà abilitata, creando una AOO denominata con la ragione sociale dell'Ente e ad essa verrà attribuito un codice; descrizione e codice possono essere modificati dall'operatore tramite la procedura ENTI PROTOCOLLO/A.O.O. della Gestione Tabelle (operazione permessa solo prima del 1° invio). Tutti i protocolli già registrati e tutti quelli successivi faranno capo a tale AOO.
2. Nel caso in cui invece l'Ente abbia già in uso la funzione 'Enti protocollo', si dovrà decidere:
    a. se sono realmente AOO diverse: attivare i parametri 'Attivo' ed inserire il codice dell' 'Area Organizzativa Omogenea' (codice identificativo alfanumerico presente sull'IPA, sia che si tratti di quello proposto dalla stessa amministrazione in sede di iscrizione, sia che si tratti di quello assegnato alla medesima dall'Indice PA in caso di non univocità) per procedere con l'usuale protocollazione (più AOO corrispondono a più registri di protocollo con numerazione progressiva separata).
    b. se NON si tratta di AOO diverse: è necessario crearne una nuova (l'unica che risulterà Attiva) con la quale iniziare a protocollare dal 12/10/2015 con il nr.1. Inoltre si fa notare che la data proposta in automatico dal sistema è quella impostata sul PC Server e non sui singoli PC collegati alla rete. È reso quindi obbligatorio effettuare le registrazioni in Ordine Cronologico.

### 6.7 Disposizioni riferite al sistema software adottato

**MODIFICA PROTOCOLLI:** 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.

**STAMPATO:** il campo 'Stampato' viene gestito automaticamente in base all'invio dei dati al sistema di conservazione.

**NUMERAZIONE**: l'unica numerazione ammessa è quella PROGRESSIVA e già descritta.

**PROTOCOLLAZIONE MAIL PEC:** Come sopra descritto, le PEC vengono protocollate riportando nell'oggetto il contenuto descrittivo della mail ed allegando come file le notifiche/allegati che accompagnano la PEC. Con un unico numero di protocollo è quindi possibile gestire tutto il processo.

**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.

**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).

**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.

### 6.8 Creazione/invio files

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:

1. **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)***.
2. **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.

# 7 DISPOSIZIONI FINALI

## 7.1 Modalità di approvazione e aggiornamento del manuale

La PA adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico e del consulente individuato nella Società CBA Informatica Srl e nella Società Seen Solution Srl..
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.

## 7.2 Disposizioni abrogate

Con l'entrata in vigore del presente manuale sono abrogate tutte le disposizioni interne all'AOO (procedure, regolamenti, prtiche) nelle parti contrastanti con lo stesso.

## 7.3 Pubblicità del presente Manuale

II presente manuale è disponibile alla consultazione del pubblico tramite pubblicazione sul sito internet istituzionale (www.apspavio.it).

## 7.4 Operatività del presente manuale

II presente manuale è operativo a decorrere dall'approvazione da parte del Consiglio di Amministrazione dell'A.P.S.P..

Il Responsabile della gestione documentale
Dott. Andrea Zencher

# Appendice A: Metodi del WS del Sistema documentale utilizzabili[6]

***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>
             ...
```

[6] Tutte le session_id indicate si intendono restituite all'atto del login, sono omesse per semplicità le operazioni di login e logout. Il login si intende effettuato con le credenziali della PA

```
                    </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]">
        <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>

        …
```

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>
        <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 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[7] i metadati:

- <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

[7] come indicato nel paragrafo 3.2 della Circolare Agid

    - 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[8]
- Data
- Classe_documentale[9]
- Codice_ufficio_pa
- Codice_fiscale_pa
- Partita_iva_pa

[8] Come indicato nell'omonimo tag dell'indice.
[9] Come indicato nel tag <docClass> dell'indice

## 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[10] |
|---|---|
| • Ragione sociale<br>• Partita IVA<br>• Codice Fiscale<br>• Codice ufficio<br>• Indirizzo<br>• CAP<br>• Comune<br>• Provincia<br>• Stato | • Nome<br>• Cognome<br>• Codice fiscale<br>• Telefono<br>• Email<br>• Pec[11]<br>• Sesso<br>• Data di nascita<br>• Comune di nascita<br>• Provincia di nascita<br>• Stato di nascita<br>• Indirizzo di residenza<br>• CAP di residenza<br>• Comune di residenza<br>• Provincia di residenza<br>• Stato di residenza |

10 Tale figura rappresenta il Resp. Conservazione/Resp. Produttore all'interno della PA che, nello specifico, coincide con il Resp. della Gestione Documentale come da D.P.C.M. del 03/12/2013

11 Verrà usata quella di Seen Solution