

*Manuale di gestione del protocollo*  
*Autore: Demartin Fabrizio*  
*Data: 12/10/2015*

**APSP SAN GAETANO**  
**VIA E. SOTTASS N° 11**  
**38037 PREDAZZO (TN)**

**MANUALE DI  
GESTIONE DEL  
PROTOCOLLO  
INFORMATICO E DEI  
DOCUMENTI  
DELL'ARCHIVIO**  
*Versione 1.0*

*A.P.S.P.*  
**"SAN GAETANO"**

**Redatto, verificato ed approvato da:**

**Nominativo:**

**Funzione:**

*Demartin Fabrizio*

Responsabile Gestione Documentale

*Nicola Savino*

Consulente per la Gestione Documentale e la  
Redazione del presente Manuale

## SOMMARIO

<b>1) PRINCIPI GENERALI</b> .....	4
1.1 Premessa.....	4
1.2 Definizioni e norme di riferimento.....	4
1.3 Aree organizzative omogenee.....	5
1.4 Servizio per la gestione informatica del protocollo.....	5
1.5 Tutela dei dati personali.....	6
1.6 Caselle di Posta Elettronica.....	6
1.7 Accreditamento dell'AOO all'IPA.....	6
<b>2) PIANO DI SICUREZZA PER LA GESTIONE DEL PROTOCOLLO INFORMATICO</b> .....	6
2.1 Obiettivi del piano di sicurezza.....	7
2.2 Formazione dei documenti – Aspetti attinenti alla sicurezza.....	7
• Componente logica della sicurezza.....	8
• Componente infrastrutturale della sicurezza.....	8
<b>3) CONSERVAZIONE DEI DOCUMENTI PER LA GESTIONE DEL PROTOCOLLO INFORMATICO</b> .....	8
• Descrizione della soluzione.....	8
• Operazioni cliente.....	9
• Richiesta di attivazione di una nuova PA.....	9
• Caricamento dei registri.....	9
• Richiesta di stato.....	9
• Appendice A: Metodi del WS del sistema documentale utilizzati dal cliente.....	10
• Ricerca della cartella "Registro di Protocollo Informatico".....	10
• Upload dei documenti.....	11
• Collegamento dei documenti.....	15
• Verifica dello stato di un documento.....	15
• Appendice B: XML dell'indice.....	17
• Appendice C:XML della segnatura.....	18
• Appendice D: Tipi e metadati definiti nel Sistema documentale.....	18
• Appendice E: Dati anagrafici per attivazione PA.....	20

<b>4) MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER SCAMBIO DI DOCUMENTI.....</b>	<b>21</b>
4.1 Documento ricevuto.....	21
4.2 Documento inviato.....	22
4.3 Documento interno.....	22
4.4 Il documento analogico - cartaceo.....	22
4.5 Formazione del registro di protocollo e dei documenti soggetti a protocollo.....	22
4.6 Posta elettronica certificata.....	24
<b>5) ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE.....</b>	<b>24</b>
5.1 Documenti esclusi.....	24
5.2 Documenti soggetti a registrazione particolare.....	25
<b>6) SISTEMA DI SOFTWARE DI CLASSIFICAZIONE, FASCICOLAZIONE E DI PROTOCOLLO INFORMATICO.....</b>	<b>25</b>
• Ricerca protocolli.....	26
• Raggruppamento esibenti/argomenti.....	26
• Gestione multipla inserimento protocolli.....	26
• Protocollo informatico pubblica amministrazione.....	27
• Creazione/modifica password d'accesso.....	27
• Area Organizzativa Omogenea (AOO) - Enti interni.....	27
• Modifica protocolli.....	28
• Protocollo mail PEC.....	28
• File.....	29
• Log.....	29
• Terminologia.....	29
• Creazione/invio file.....	29
<b>7) DISPOSIZIONI FINALI.....</b>	<b>30</b>
• Modalità di approvazione e aggiornamento manuale.....	30
• Regolamenti abrogati.....	30
• Pubblicità del presente manuale.....	30
• Operatività del presente manuale.....	30

## **PRINCIPI GENERALI**

### **1.1 Premessa**

Il 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).

Di seguito viene indicata l'Area Organizzativa Omogenea di questa Pubblica Amministrazione :

#### ***A.P.S.P. "San Gaetano"***

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.

### **1.2 Definizioni e norme di riferimento**

Ai fini del presente manuale si intende per:

- **"amministrazione"**, A.P.S.P. SAN GAETANO
- **"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 verranno spiegati man mano nell'argomentazione successiva.

### **1.3 Aree Organizzative Omogenee**

Per la gestione dei documenti la PA 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 una sola Area.

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

Nella 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**),

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 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, imm modificabile e visualizzabile.

### **1.5 Tutela dei dati personali**

La PA 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 si dota di almeno una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita.

**[apspsanqaetano@legalmail.it](mailto:apspsanqaetano@legalmail.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.

Il codice identificativo delle 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 PA di avere il codice di riferimento che verrà gestito ed inserito nel registro di protocollo, sottoposto a conservazione.

## **2. PIANO DI SICUREZZA PER LA GESTIONE DEL PROTOCOLLO INFORMATICO**

Si rimanda alle "Procedure in materia di privacy, misure di sicurezza e trattamento dati personali", oggetto di revisione annua

## 2.1 Obiettivi del piano di sicurezza

Le "Procedure in materia di privacy, misure di sicurezza e trattamento dati personali" garantisce che:

- i documenti e le informazioni trattate dall'AOO sono disponibili, integre e riservate e che nessun altro utente non autorizzato possa accedervi;
- i dati personali comuni, sensibili e/o giudiziari vengono 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.
- Il presente documento è stato oggetto di verifica ed analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono i software e l'hardware utilizzato per il protocollo;
- Garantire che il protocollo informatico e tutti i flussi ad esso associato, vengono gestiti secondo quanto richiesto dal Dlgs 196/2003 e che sia garantito il piano della sicurezza descritto dal responsabile privacy.

## 2.2 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 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.

### **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 dalle 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.

### **Componente infrastrutturale della sicurezza**

Presso la PA, sono presenti i seguenti impianti:

- antincendio;
- luci di emergenza;
- continuità elettrica;

### **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.

#### **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 segnature 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 sabato raccoglie tutti gli indici caricati il giorno lavorativo precedente 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".

## **Operazioni cliente<sup>1</sup>**

### **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 della PA.

- cerca la cartella con nome "Registro di Protocollo Informativo" all'interno della cartella root della PA
- effettua l'upload dei seguenti file<sup>2</sup>

- pdf di tipo "Registro\_Giornaliero\_di\_Protocollo"

- xml di tipo "Segnatura\_di\_Protocollo"<sup>3</sup>

- pdf di tipo "Log\_di\_Registro"

- 3 xml di tipo "Indice\_del\_Pacchetto\_di\_Versamento"<sup>4</sup> 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.

<sup>1</sup> la lista dei metodi del ws che il cliente dovrà utilizzare si trova nell'appendice A

<sup>2</sup> Il set di metadati per Ktreedoc è indicato nell'appendice D

<sup>3</sup> i dati da inserire nel file di segnatura sono indicati nell'appendice C

<sup>4</sup> informazioni più dettagliate sugli indici si trovano nell'appendice B

- "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:<sup>5</sup>

### 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>
```

<sup>5</sup> tutte le sessioni 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

```
<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/">
        <b>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>
  <documenttype
xsi:type="xsd:string">Registro_Giornaliero_Di_Protocollo</docum
enttype>
  <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>
  </return>
</SOAP-ENV:add_base64_document_with_metadataResponse>
</SOAP-ENV:Body>
...
```

### 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_azienza_a.pdf</title>  
        <document_type  
xsi:type="xsd:string">Registro_Giornaliero_di_Protocollo</document  
_type>  
        <filename  
xsi:type="xsd:string">20150929_azienza_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_azienza_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 <sup>6</sup> 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\_prodotto\_2
  - Cognome\_soggetto\_prodotto\_2
  - Codice\_fiscale\_soggetto\_prodotto\_2

<sup>6</sup> come indicato nel paragrafo 3.2 di [questa](#) circolare Agid

- 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 identificativo PA
- Codice identificativo 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"

Manuale di gestione del protocollo  
Autore: Demartin Fabrizio  
Data: 12/10/2015

**APSP SAN GAETANO**  
VIA E. SOTTASS N° 11  
**38037 PREDAZZO (TN)**

### 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 <sup>9</sup>
<ul style="list-style-type: none"><li>● Ragione sociale</li><li>● Partita IVA</li><li>● Codice Fiscale</li><li>● Codice ufficio</li><li>● Indirizzo</li><li>● CAP</li><li>● Comune</li><li>● Provincia</li><li>● Stato</li></ul>	<ul style="list-style-type: none"><li>● Nome</li><li>● Cognome</li><li>● Codice fiscale</li><li>● Telefono</li><li>● Email</li><li>● Pec<sup>10</sup></li><li>● Sesso</li><li>● Data di nascita</li><li>● Comune di nascita</li><li>● Provincia di nascita</li><li>● Stato di nascita</li><li>● Indirizzo di residenza</li><li>● CAP di residenza</li><li>● Comune di residenza</li><li>● Provincia di residenza</li><li>● Stato di residenza</li></ul>

<sup>9</sup> Tale figura rappresenta il Resp. Conservazione/Resp. Produttore all'interno della PA che, nello specifico, coincide con il Resp. della Gestione Documentale come d D.P.C.M. del 03/12/2013

<sup>10</sup> verrà usata quella di Seen Solution

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

Il presente capitolo spiega in modo sufficiente ma esaustivo il mondo in cui i documenti vengono gestiti dalla PA.

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 avverrà l'11 Agosto 2016, il documento amministrativo può essere disponibile anche nella forma analogica 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 di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato:

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

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telegramma;
4. per fax
5. a mano

Il documento analogico ricevuto viene protocollato e archiviato nel fascicolo di competenza, mentre il documento informatico viene stampato, protocollato e archiviato come il documento analogico.

#### **4.2 Documento inviato**

I documenti informatici, compresi di eventuali allegati, sono inviati alle PA, se possibile, per mezzo della sola posta elettronica certificata. Per tutti gli altri destinatari, dove non sia possibile l'invio con posta certificata, il documento viene spedito con posta elettronica, a mezzo posta convenzionale o raccomandata, tramite corriere o a mano.

#### **4.3 Documento interno**

I documenti interni sono prodotti con tecnologie informatiche con rilevanza amministrativa giuridico-probatoria, o con tecnologie analogiche: in questo caso il documento viene creato con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e protocollato.

I documenti interni e le procedure per lo svolgimento delle attività lavorative vengono caricate nell'apposito "software delle procedure", visibile a tutti i dipendenti sui Pc in dotazione. I dipendenti vengono informati con messaggio personale sulla Cartella socio-sanitaria informatizzata delle modifiche fatte e delle eventuali nuove procedure caricate.

#### **4.4 Il documento analogico - cartaceo**

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

#### **4.5 Formazione del registro di protocollo e dei documenti 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 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 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.

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.

#### **4.6 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.

I messaggi di ritorno, 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 i documenti di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 come riportato

nell'allegato 11, e i seguenti documenti : Deliberazioni del Consiglio di amm.ne, Determine del Direttore e Provvedimenti del Presidente, richieste di visite fiscali, materiale pubblicitario o pubblicizzazione di incontri, eventi o manifestazioni, giornali e riviste, abbonamenti a giornali e riviste, materiale statistico, certificati medici ecc.

## **5.2 Documenti soggetti a registrazione particolare**

Nessun documento è soggetto a registrazione particolare.

## **6. SISTEMA DI 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 dà inizio 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/fornitori 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: attinge dall'anagrafica dei dipendenti del software Stipendi/Presenze/Turni.

Sarà inoltre possibile, qualora sia gestito e richiesto, sia le SPESE e TIPOLOGIA DI SPEDIZIONE, sia gli uffici di competenza del documento protocollato.

#### • 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

#### • Raggruppamento esibenti/argomenti

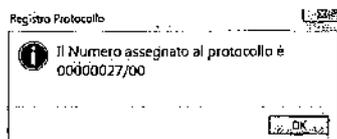
La funzione consente di raggruppare Esibenti e/o Argomenti per una razionalizzazione dei dati gestiti nel corso degli anni.

E' 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.

#### • 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.

#### • Protocollo informatico pubblica amministrazione

Il sistema di protocollo informatico assicura:

- a) **univoca identificazione** ed autenticazione degli utenti;
- b) la **protezione delle informazioni** relative a ciascun utente nei confronti degli altri;
- c) la garanzia di accesso alle risorse esclusivamente agli **utenti abilitati**;
- d) 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:

- α) il **controllo differenziato dell'accesso** alle risorse del sistema per ciascun utente o gruppo di utenti;
- β) 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**.

#### • 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).

#### • Area organizzativa omogenea (AOO) – Enti interni

Il registro protocollo deve far riferimento all'Area Organizzativa Omogenea (AOO) dell'Ente.

Nel caso in cui vi siano più AOO, ognuna 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.'

*Possano 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. E' reso quindi obbligatorio effettuare le registrazioni in Ordine Cronologico.

#### • **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 inviati 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.

#### • Creazione/invio files

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

\* **File METADATI.xml del giorno richiesto :** riassume brevemente il contenuto dei documenti in modo da facilitarne l'identificazione.

## 7) DISPOSIZIONI FINALI

### • 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.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti al miglioramento in termini di efficacia, efficienza e trasparenza.
- Inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

### • Regolamenti abrogati

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

### • Pubblicità del presente Manuale

Il presente manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento. Inoltre copia del presente manuale è:

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

### • Operatività del presente manuale

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



**Responsabile Gestione Documentale**  
Demartin dott. Fabrizio

A handwritten signature in black ink, appearing to be "Demartin".