



COMUNE DI SANTA GIUSTINA IN COLLE  
Provincia di Padova

# **Manuale di Gestione del Protocollo Informatico, dei Documenti e dell'Archivio**

(artt. 3, 4 e 5 DPCM 03.12.2013)

## SOMMARIO

<b>SEZIONE I. DISPOSIZIONI GENERALI.....</b>	<b>2</b>
1.1 Ambito di applicazione .....	4
1.2 Definizioni dei termini .....	4
1.3 Area organizzativa omogenea .....	4
1.4 Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi .....	4
1.5 Unicità del protocollo informatico .....	4
1.6 Modello operativo adottato per la gestione dei documenti .....	5
1.7 Modalità di gestione del protocollo informatico .....	5
<b>SEZIONE II. FORMAZIONE DEI DOCUMENTI.....</b>	<b>6</b>
2.1 I documenti del Comune e modalità di formazione dei documenti e contenuti minimi	6
2.2 Formato dei documenti informatici.....	7
2.3 Sottoscrizione dei documenti informatici .....	7
2.4 Verifica delle firme digitali.....	8
2.5 Tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche .....	8
2.6 Formazione e gestione delle minute e dei documenti base .....	8
<b>SEZIONE III. RICEZIONE DEI DOCUMENTI.....</b>	<b>9</b>
3.1 Ricezione dei documenti su supporto cartaceo .....	9
3.2 Ricezione dei documenti informatici .....	9
3.3 Ricevute attestanti la ricezione dei documenti .....	10
3.4 Apertura della posta .....	10
<b>SEZIONE IV. REGISTRAZIONE DEI DOCUMENTI.....</b>	<b>10</b>
4.1 Documenti soggetti a registrazione di protocollo.....	10
4.2 Documenti non soggetti a registrazione di protocollo.....	10
4.3 Registrazione di protocollo dei documenti ricevuti e spediti .....	11
4.4 Registrazione dei documenti interni.....	12
4.5 Segnatura di protocollo .....	12
4.6 Annullamento delle registrazioni di protocollo.....	13
4.7 Differimento dei termini di protocollazione.....	13
4.8 Registro giornaliero e annuale di protocollo.....	13
4.9 Requisiti minimi di sicurezza dei sistemi di protocollo informatico.....	13
4.10 Registro di emergenza.....	14
<b>SEZIONE V. DOCUMENTAZIONE PARTICOLARE.....</b>	<b>15</b>
5.1 Registrazione particolare (repertori) .....	15
5.2 Documentazione di gare d'appalto .....	15
5.3 Documenti su supporto cartaceo indirizzati nominalmente al personale dell'ente, lettere anonime e documenti non firmati.....	15
5.4 Corrispondenza con più destinatari e copie per conoscenza .....	15
5.5 Allegati.....	16
5.6 Documenti pervenuti per errore.....	16
5.7 Oggetti plurimi .....	16
5.8 Gestione della posta elettronica .....	16
5.9 Produzione di copie e duplicati .....	17
5.10 Trasmissioni telematiche.....	19
<b>SEZIONE VI. ASSEGNAZIONE DEI DOCUMENTI.....</b>	<b>20</b>

6.1 Assegnazione e consegna.....	20
6.2 Modifica delle assegnazioni.....	20
<b>SEZIONE VII. CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI .....</b>	<b>21</b>
7.1 Classificazione dei documenti.....	21
7.2 Formazione e identificazione dei fascicoli.....	21
7.3 Processo di formazione dei fascicoli .....	22
7.4 Fascicolo ibrido.....	22
7.5 Archivio corrente e di deposito .....	22
<b>SEZIONE VIII. SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO.....</b>	<b>25</b>
8.1 Spedizione dei documenti analogici.....	25
8.2 Spedizione dei documenti informatici.....	25
<b>SEZIONE IX. SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO .....</b>	<b>26</b>
9.1 Documenti soggetti a scansione .....	26
9.2 Processo di scansione.....	26
<b>SEZIONE X. CONSERVAZIONE E TENUTA DEI DOCUMENTI.....</b>	<b>27</b>
10.1 Conservazione dei documenti informatici.....	27
10.2 Selezione e conservazione dei documenti.....	27
<b>SEZIONE XI. PIANO DI SICUREZZA.....</b>	<b>28</b>
11.1 Obiettivi del Piano di sicurezza.....	28
11.2 Formazione dei documenti informatici – aspetti di sicurezza.....	28
11.3 Gestione delle registrazioni di protocollo e di sicurezza.....	28
11.4 Accesso ai documenti informatici .....	29
11.5 Utenti interni alla AOO .....	29
11.6 Profili utente e responsabilità.....	29
11.7 Conservazione dei documenti informatici.....	30
<b>SEZIONE XII. ACCESSO.....</b>	<b>31</b>
12.1 Accessibilità da parte degli utenti appartenenti all'Amministrazione.....	31
12.2 Accesso esterno.....	31
<b>SEZIONE XIII. APPROVAZIONE, REVISIONE E PUBBLICAZIONE .....</b>	<b>32</b>
13.1 Approvazione.....	32
13.2 Revisione.....	32
13.3 Pubblicazione.....	32
 <b>ALLEGATI.....</b>	 <b>33</b>

## SEZIONE I. DISPOSIZIONI GENERALI

### *1.1 Ambito di applicazione*

Il presente manuale è adottato ai sensi degli articoli 3, 4 e 5 del DPCM 03.12.2013 per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti dell'Amministrazione.

### *1.2 Definizioni dei termini*

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al glossario allegato al DPCM 3.12.2013 (Allegato n. 2).

### *1.3 Area organizzativa omogenea (AOO)*

Ai fini della gestione dei documenti è individuata una sola area organizzativa omogenea denominata **Comune di Santa Giustina in Colle** composta dall'insieme di tutte le sue unità organizzative e dotata di un unico sistema di protocollo (Allegato 1). Il codice identificativo dell'AOO attribuito dall'Indice delle Pubbliche Amministrazioni (/www.indicepa.gov.it) è **c\_i207**. Per qualsiasi informazione statistica relativa all'Amministrazione si rimanda alle pagine del sito: [www.comunesgcolle.gov.it](http://www.comunesgcolle.gov.it)

### *1.4 Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi*

Nell'ambito dell'Area Organizzativa Omogenea, ai sensi dell'articolo 61, comma 1, del D.P.R. 445/2000, è istituito il Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi (Allegato 1). Il servizio, ai sensi dell'articolo 61, comma 3, del D.P.R. 445/2000 ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata dell'Amministrazione, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento. Il Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi" è il Responsabile del 1° Settore "Economico-Finanziario-Affari Generali".

### *1.5 Unicità del protocollo informatico*



La numerazione delle registrazioni di protocollo è unica, progressiva e corrisponde all'anno solare, tuttavia a norma dell'articolo 53, comma 5 del D.P.R. 445/ 2000 sono possibili registrazioni particolari (Allegato n. 3). L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Allegato n. 3). Ad ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

#### *1.6 Modello operativo adottato per la gestione dei documenti*

Per la gestione dei documenti è adottato un modello operativo parzialmente decentrato che prevede la partecipazione attiva di più soggetti ed uffici utenti abilitati a svolgere soltanto le operazioni di loro competenza; le abilitazioni sono rilasciate dal Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi".

#### *1.7 Modalità di gestione del protocollo informatico*

Il protocollo informatico del Comune di Santa Giustina in Colle è operativo dal 2/2/2004 ed utilizza il software gestionale fornito dalla ditta Kibernetes srl e denominato "Protocollo e Atti". L'applicativo utilizzato è stato inserito nel settembre 2014 nel catalogo nazionale dell'Agenzia per l'Italia Digitale, presso la Presidenza del Consiglio dei Ministri, ai sensi dell'art. 24 quater comma 2 del D.L. 90/2014 convertito in Legge 114/2014. Il manuale di utilizzo è fornito dalla ditta fornitrice del software (Allegato 6). Dalle registrazioni di protocollo è possibile estrarre sempre evidenza analogica.

L'ufficio Protocollo posto all'interno del settore "Economico-Finanziario-Affari Generali" provvede al ricevimento ed alla protocollazione di tutta la corrispondenza in arrivo indirizzata al Comune di Santa Giustina in Colle ed alle incombenze di archiviazione e tenuta dell'archivio nonché alla spedizione della corrispondenza. I dati in uscita sono gestiti dai singoli uffici assegnati alle Unità Organizzative (U.O.). Le U.O. ed i singoli servizi assegnati alle U.O. hanno la visualizzazione esclusivamente delle registrazioni di protocollo assegnate, ai sensi dell'art. 11 del D.Lgs 196/2003. Il software traccia l'autore di ogni registrazione.

## SEZIONE II. FORMAZIONE DEI DOCUMENTI

### *2.1 I documenti del Comune e modalità di formazione dei documenti e contenuti minimi*

Per documento amministrativo si intende una rappresentazione comunque formata del contenuto di atti detenuti dal Comune, indipendentemente dalla loro natura pubblicistica o privatistica, utilizzati ai fini dell'attività amministrativa.

Per documenti del Comune si intendono i documenti prodotti, spediti e ricevuti, o comunque acquisiti secondo le modalità previste dalla normativa vigente, dagli organi e dagli uffici nello svolgimento della loro attività istituzionale.

Tali documenti, connessi da speciale vincolo originario, necessario e determinato, riconosciuto quale vincolo archivistico, costituiscono l'Archivio del Comune.

Ogni documento deve trattare un solo oggetto, deve essere predisposto utilizzando un linguaggio chiaro e comprensibile, evitando l'uso di forme e costruzioni involute, sigle e locuzioni ambigue. Particolare cura andrà attribuita anche all'"oggetto", che dovrà essere una equilibrata sintesi del contenuto, redatto secondo forme normalizzate, evitando rinvii e riferimenti, che pregiudichino la comprensione del testo.

I documenti del carteggio amministrativo in base allo stato di trasmissione si distinguono in:

- **documenti in arrivo** (in entrata): documenti con rilevanza giuridico-probatoria, prodotti da altri soggetti e acquisiti dal Comune nell'esercizio delle sue funzioni e per lo svolgimento delle proprie attività
- **documenti in partenza** (in uscita): documenti, con rilevanza giuridica-probatoria, prodotti dal personale del Comune nell'esercizio delle sue funzioni e nello svolgimento delle attività amministrative e spediti a soggetti differenti
- **documenti interni**: documenti prodotti all'interno di ogni Settore oppure scambiati fra i diversi Settori. Si distinguono in documenti informali di preminente carattere informativo, documenti preparatori o accompagnatori o propedeutici formati o acquisiti durante lo svolgimento delle attività interlocutoria e conoscitiva e documenti formali di preminente carattere giuridico-probatorio, con rilevanza procedimentale, redatti dai settori nell'esercizio delle proprie funzioni al fine di documentare fatti, stati o qualità inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative da parte di terzi.

Le modalità di formazione dei documenti, del loro contenuto e della loro struttura sono determinate da quanto previsto dal presente Manuale; per quanto riguarda i documenti informatici la loro produzione è regolata sulla base di modelli standard presenti nel sistema informatico di gestione documentale. Il contenuto minimo deve comunque garantire la presenza delle seguenti informazioni:

- denominazione dell'amministrazione;
- indicazione del settore, servizio o ufficio che ha prodotto il documento;
- indirizzo completo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica dell'ente, indicazione sito web istituzionale);

- data: luogo, giorno, mese, anno;
- destinatario, per i documenti in partenza
- oggetto del documento, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- numero di protocollo;
- testo;
- estremi identificativi del responsabile del procedimento (L. 241/ 1990);
- sottoscrizione autografa o elettronico/ digitale del Responsabile.

I documenti cartacei devono essere prodotti in un numero di originali predefiniti, quanti sono i destinatari più un esemplare da conservare nel fascicolo relativo all'affare o al procedimento.

## *2.2 Formato dei documenti informatici*

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Secondo le norme del CAD, il documento informatico soddisfa il requisito legale della forma scritta solo se è sottoscritto con firma digitale o altro tipo di firma elettronica avanzata.

Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, inviati/ricevuti all'interno o all'esterno, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

E' facoltà di ogni Responsabile di Settore prendere in carico in forma ufficiale e sottoporre a protocollazione i documenti pervenuti dall'esterno alle singole mail degli uffici, e non alla casella di posta elettronica istituzionale dell'Ente.

Di norma devono essere prese in carico (assunte al protocollo dell'ente) le mail che contengono:

- Segnalazioni da parte di cittadini che si sono identificati
- Inviti a riunioni
- Documenti che rientrano o che possono dare avvio a procedimenti amministrativi e per i quali non è prevista obbligatoriamente trasmissione a mezzo PEC.

In tal caso la decorrenza dei termini è data dalla registrazione di protocollo e non dall'arrivo all'ufficio preposto.

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale o avanzata, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, come riportato sul sito dell'Agenzia per l'Italia Digitale ([www.agid.gov.it](http://www.agid.gov.it)), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. A titolo d'esempio si utilizzano preferibilmente: PDF e PDF/ A.

## *2.3 Sottoscrizione dei documenti informatici*

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale o avanzata conforme alle disposizioni di legge. L'assegnazione dei dispositivi di firma compete al Responsabile del Settore Economico-Finanziario-Affari Generali, il quale provvede ad autorizzare l'utilizzo della firma digitale o avanzata ed è responsabile del controllo della scadenza dei certificati

di firma e del loro eventuale rinnovo, salva la possibilità di rinnovo tramite dispositivo di firma da parte del titolare di firma stesso..

#### *2.4 Verifica delle firme digitali*

La sequenza delle operazioni previste per la verifica di integrità del documento firmato digitalmente, è la seguente:

- apertura del file firmato;
- verifica della validità del certificato e della corrispondenza delle impronte del documento.

Queste attività sono realizzate mediante un'applicazione appositamente fornita da parte dell'ente fornitore dei certificati di firma digitale in dotazione all'Ente (si rinvia alla seguente pagina <http://www.digitpa.gov.it/firme-elettroniche/software-di-verifica-della-firma-digitale>, dove si può trovare una lista di software che possono essere usati per la verifica della firma).

Spetta ai responsabili di procedimento verificare l'integrità dei documenti firmati digitalmente di propria competenza.

#### *2.5 Tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche*

Per quanto riguarda un quadro generale di casi che possono creare dubbi sull'opportunità della protocollazione, si rimanda alla Sezione 5 "Documentazione particolare".

#### *2.6 Formazione e gestione delle minute e dei documenti base*

Per ogni documento destinato a essere spedito sono scritti due o più esemplari quanti sono i destinatari, oppure un documento base nel caso in cui si producano documenti seriali a contenuto e destinatario diversificati (per quanto riguarda la gestione dei documenti a destinatario multiplo si rimanda alla Sezione 5 "Documentazione particolare"). Uno di questi esemplari classificato si conserva nel fascicolo dopo che sono state eseguite le operazioni descritte successivamente. L'esemplare che si conserva nel fascicolo (minuta) può avere la dicitura "Copia" e deve contenere il numero di protocollo assegnato.

## SEZIONE III. RICEZIONE DEI DOCUMENTI

### 3.1 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

- a) il servizio postale;
- b) la consegna diretta agli uffici, ai funzionari, o agli uffici utente abilitati presso l'amministrazione al ricevimento della documentazione;
- c) gli apparecchi telefax.

**I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione.** Quelli arrivati via telefax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei; in presenza di un sistema informatico che ne consenta l'acquisizione in formato elettronico (fax management) si applicano le procedure previste per la ricezione dei documenti informatici. In sede di conversione del D.L. n. 69/2013, la Legge n. 98/2013, introducendo il comma 1 bis all'articolo 14, ha stabilito l'esclusione della trasmissione via fax delle comunicazioni di documenti tra pubbliche amministrazioni. Tale comma 1-bis modifica l'articolo 47 del Codice dell'amministrazione digitale (D.Lgs. 82/2005) escludendo la trasmissione di documenti a mezzo fax da parte della PA ad altre P.A. Il fax per l'invio di documenti ad altre PA potrà quindi essere utilizzato solo in casi eccezionali di malfunzionamenti del sistema informatico.

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

Non è pertanto consentito, in nessun caso, l'utilizzo di un unico numero di protocollo per il documento in arrivo e il documento in partenza. La documentazione che non è stata registrata in arrivo o in partenza viene considerata giuridicamente inesistente per l'Amministrazione.

La corrispondenza indirizzata alla cortese attenzione del personale è regolarmente aperta e registrata al protocollo.

Non è ammessa la ricezione di corrispondenza di carattere personale; il Servizio di Protocollo è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.

A chi richieda ricevuta di un documento consegnato, compatibilmente con le possibilità del servizio, verrà consegnata l'apposita stampa ottenibile dal sistema informatico.

### 3.2 Ricezione dei documenti informatici

Un documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, può essere recapitato:

- a mezzo posta elettronica certificata (PEC) o equivalente;
- su supporto rimovibile (quale, ad esempio, CD ROM, DVD, pen drive, etc.) consegnato direttamente all'ufficio protocollo, all'ufficio competente il procedimento o inviato per posta

convenzionale o corriere. In questo caso, l'ufficio ricevente verifica la compatibilità del supporto presentato e la leggibilità dello stesso.

La ricezione dei documenti informatici è assicurata tramite una casella di posta elettronica certificata integrata con il sistema informatico e accessibile solo all'ufficio preposto alla registrazione di protocollo. Gli indirizzi della casella di posta elettronica istituzionale e della casella di posta elettronica certificata sono reperibili sul sito web dell'amministrazione. ([www.comunesgcolle.gov.it](http://www.comunesgcolle.gov.it))

Il Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi" provvede a renderlo pubblico e a trasmetterlo all'Agenzia per l'Italia digitale ai sensi dell'articolo 12 del D.P.C.M. 3 dicembre 2013. I documenti informatici eventualmente pervenuti ad altri indirizzi mail, devono essere inoltrati all'indirizzo di posta elettronica istituzionale dell'Ente per la registrazione.

### *3.3 Ricevute attestanti la ricezione dei documenti*

La ricevuta della consegna di un documento cartaceo può essere costituita dalla fotocopia del primo foglio del documento stesso con apposizione del timbro di protocollo. Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico per i documenti trasmessi tramite PEC.

Per i documenti in arrivo già registrati può essere rilasciata apposita ricevuta con gli estremi della segnatura ottenuta tramite la procedura informatica di protocollo.

### *3.4 Apertura della posta*

Il Servizio Protocollo apre tutta la corrispondenza cartacea pervenuta all'Ente salvo i casi particolari specificati nella Sezione n. 5, compresa la posta elettronica istituzionale e la PEC.

Le buste dei documenti pervenuti si inoltrano insieme ai documenti quando contengano dati necessari al procedimento.

## **SEZIONE IV. REGISTRAZIONE DEI DOCUMENTI**

### *4.1 Documenti soggetti a registrazione di protocollo*

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.

### *4.2 Documenti non soggetti a registrazione di protocollo.*

Sono esclusi dalla registrazione di protocollo:

- gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico - amministrativa presente o futura;
- tutte le comunicazioni e tutti i documenti aventi rilevanza esclusivamente interna e di carattere preminentemente informativa, siano essi predisposti in forma cartacea che in formato elettronico, salva diversa indicazione del Responsabile di Settore;
- tutti quei documenti già soggetti a registrazione particolare da parte dell'ente (Allegato n. 3)

#### *4.3 Registrazione di protocollo dei documenti ricevuti e spediti*

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e numero di protocollo dei documenti ricevuti, se disponibili;
- f) impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- g) classificazione: categoria, classe, (Titolario - allegato 6);
- h) assegnazione.

Inoltre possono essere aggiunti:

- i) allegati (numero e descrizione);
- j) estremi provvedimento differimento termini di registrazione;
- k) mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere, fax ecc.);
- l) livello di riservatezza;
- m) elementi identificativi del procedimento amministrativo, se necessario.

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per: documenti relativi a vicende o a fatti privati o particolari (dati sensibili come definiti dal Codice in materia di protezione dei dati personali, art. 4, comma 1, lettera d). I documenti registrati con tali forme appartengono al protocollo particolare (o “protocollo riservato”), costituito dalle registrazioni



sul protocollo informatico unico il cui accesso è autorizzato solo alle persone indicate, in rapporto alle tipologie documentarie e ai procedimenti amministrativi.

Le tipologie di documenti da registrare nel protocollo particolare sono individuate dal Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” su indicazione del Responsabile di Settore o del Segretario Comunale per la tipologia. La documentazione da sottoporre a protocollo particolare può essere individuata con l’apposizione della firma o nota autografa sul documento da registrare.

Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti e procedimenti amministrativi, ma la visibilità sarà inibita con la dicitura “riservato” e sarà consentita solo alle persone autorizzate.

I documenti registrati sul protocollo particolare divengono consultabili alla scadenza dei termini, se previsti, indicati dalla normativa vigente. Motivate richieste di consultazione potranno essere accolte prima della scadenza dei termini secondo le procedure previste dalla normativa vigente.

#### *4.4 Registrazione dei documenti interni*

Di norma i documenti prodotti dall'Ente a solo uso interno non vengono protocollati. Nel caso in cui sia necessario dare valenza giuridico - probatoria a documenti che costituiscono atti preparatori (pareri tecnico - legali) o per indicazione del Responsabile di Settore, essi potranno essere protocollati mediante la specifica funzione del software di protocollo.

I documenti interni sono di norma prodotti con tecnologie informatiche, mediante la specifica funzione del software.

#### *4.5 Segnatura di protocollo*

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo. La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Per i documenti informatici, i dati relativi alla segnatura di protocollo sono contenuti, un’unica volta nell’ambito dello stesso messaggio, in un file conforme alle specifiche dell’Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD). La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

Considerato che la registrazione di protocollo in uscita va effettuata dopo che il documento è stato datato e sottoscritto, il documento nativo firmato digitalmente è un file “p7m”, che non può contenere visibile al suo interno la numerazione di protocollo.

La registrazione di protocollo, in quanto operazione finale, va fatta in un momento successivo rispetto alla formazione-chiusura del documento nativo digitale e il software di protocollo che



trasmetterà tale documento con PEC o mail darà a corredo del file da trasmettere, un file di segnatura contenente tutti i dati della registrazione di protocollo.

#### *4.6 Annullamento delle registrazioni di protocollo*

Le registrazioni di protocollo possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti e con autorizzazione del Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” a seguito di motivata richiesta scritta (anche tramite e-mail) o per iniziativa dello stesso Responsabile. Le registrazioni annullate rimangono memorizzate nel registro informatico e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra gli estremi del provvedimento autorizzativo redatto dal Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi”. Il documento è conservato, all'interno del fascicolo di competenza, a cura del responsabile del procedimento. Il Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” mantiene comunque un'attività di controllo sull'operato dei responsabili di procedimento.

#### *4.7 Differimento dei termini di protocollazione*

La registrazione della documentazione pervenuta avviene nell'arco della giornata. Il Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi”, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati. Ai fini giuridici i termini decorrono dalla data di ricezione riportata sul documento analogico tramite un apposito timbro; il sistema informatico mantiene traccia del ricevimento dei documenti.

#### *4.8 Registro giornaliero di protocollo*

Il contenuto del registro giornaliero di protocollo informatico è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto, così come previsto all'art. 7, comma 5 del D.P.C.M. 3 dicembre 2013. Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

#### *4.9 Requisiti minimi di sicurezza dei sistemi di protocollo informatico*

Il sistema di Protocollo Informatico assicura:

- a) l'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 il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti e il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Le registrazioni devono essere protette da modifiche non autorizzate.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del “Codice in materia di protezione dei dati personali”, di cui al Decreto Legislativo 30 giugno 2003, n. 196.

#### *4.10 Registro di emergenza*

Il Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza, a norma dell'articolo 63 del D.P.R. 445/ 2000, su supporto cartaceo da archiviare a cura del Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” unitamente alla propria copia del registro annuale di protocollo e provvede successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico, tramite le procedure previste dal manuale operativo del sistema informatico (Allegato 9) e dalla guida all'attivazione del registro (Allegato n. 5). Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza. All'inizio di ogni anno, il Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi” provvede a istituire il registro di emergenza su supporto cartaceo (Allegato n. 5).

## SEZIONE V. DOCUMENTAZIONE PARTICOLARE

### *5.1 Registrazione particolare (repertori)*

I documenti già soggetti a registrazione particolare da parte dell'Ente (repertori), possono non essere registrati al protocollo. Il software di produzione e conservazione di questa tipologia particolare di documentazione deve consentire di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico. Ogni registrazione deve riportare necessariamente:

- a) dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- b) numero di repertorio progressivo e annuale (generato in modo non modificabile).

Per quanto riguarda i contratti, fermo restando quanto riportato ai precedenti punti a) e b), si precisa che il numero di repertorio è progressivo, ma non annuale.

Per quanto riguarda le pubblicazioni all'Albo on-line si rimanda all'apposito Regolamento.

### *5.2 Documentazione di gare d'appalto*

Le offerte di gare d'appalto o altra documentazione da consegnarsi all'Ente in busta chiusa sono registrate al protocollo. Dopo l'apertura della busta a cura dell'ufficio che gestisce la gara verrà riportato su ciascun documento contenuto il medesimo numero di protocollo assegnato alla busta.

### *5.3 Documenti su supporto cartaceo indirizzati nominalmente al personale dell'ente, lettere anonime e documenti non firmati*

La corrispondenza indirizzata nominativamente è regolarmente aperta e registrata al protocollo.

Le lettere anonime vengono regolarmente protocollate.

Le lettere con firma illeggibile vengono regolarmente protocollate.

### *5.4 Corrispondenza con più destinatari e copie per conoscenza*

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo. Se in uscita, i destinatari possono essere descritti in elenchi associati al documento.

Dei documenti analogici prodotti/ pervenuti, di cui necessita la distribuzione interna all'Ente, si faranno copie informatiche degli stessi.

### *5.5 Allegati*

Su ogni allegato è riportata la segnatura di protocollo. Il sistema informatico provvede automaticamente a registrare gli allegati di un documento elettronico.

### *5.6 Documenti pervenuti per errore*

I documenti pervenuti per errore non devono essere protocollati e restituiti al mittente. I documenti pervenuti per errore tramite PEC verranno protocollati e inoltrati al destinatario, se ben identificato, o restituiti al mittente.

### *5.7 Oggetti plurimi*

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi e pertanto da assegnare a più fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente una dall'altra.

### *5.9 Gestione della posta elettronica*

Per il corretto impiego della posta elettronica ed anche al fine di estenderne l'uso nell'ambito dell'attività amministrativa interna, si richiama quanto indicato dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie: "è sufficiente ricorrere ad un semplice messaggio di posta elettronica, ad esempio, per richiedere o concedere ferie o permessi, richiedere o comunicare designazioni in comitati, commissioni, gruppi di lavoro o altri organismi, convocare riunioni, inviare comunicazioni di servizio ovvero notizie dirette al singolo dipendente, diffondere circolari o ordini di servizio".

Ad integrazione di quanto citato, si puntualizza che la trasmissione di documenti informatici tramite la posta elettronica deve attenersi alle norme ed alle regole vigenti al fine di garantirne la validità legale ed amministrativa e la loro corretta gestione nell'ambito del sistema adottato per la classificazione, l'archiviazione e la conservazione dei documenti e dei fascicoli. In particolare, come stabilito dall'articolo 6 del Codice dell'Amministrazione Digitale, il Comune di Santa Giustina in Colle utilizza la posta elettronica certificata per ogni scambio di documenti e informazioni con tutti i soggetti interessati (pubbliche amministrazioni, imprese, professionisti e cittadini) che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.

La casella istituzionale di posta elettronica certificata, collegata con il sistema di protocollo informatico è quindi l'indirizzo elettronico ufficiale atto a ricevere messaggi da altre pubbliche amministrazioni, cittadini, professionisti ed imprese dotati di analoghi strumenti di trasmissione (PEC).

Il Comune di Santa Giustina in Colle ha adempiuto a tali obblighi dotandosi di un indirizzo di posta elettronica certificata, pubblicando tale indirizzo sulla home page del proprio sito Internet e comunicandolo all'Indice P.A. ([www.indicepa.it](http://www.indicepa.it)).

Qualora i file allegati non siano corredati di firma digitale essi verranno protocollati e successivamente inoltrati al responsabile di procedimento, che provvederà alla valutazione del contenuto del documento pervenuto.

La posta elettronica individuale non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale per i quali è prevista l'apposita casella di posta elettronica certificata.

I documenti informatici eventualmente pervenuti ad altri indirizzi mail, nel caso pervengano da altre pubbliche amministrazioni, professionisti o imprese, devono essere re-inoltrati dal mittente all'indirizzo di posta elettronica certificata dell'Ente per la registrazione, previo avviso al mittente da parte del personale dell'Ente che ha erroneamente ricevuto la mail.

Nel caso in cui i documenti informatici pervengano dai cittadini privi di posta elettronica certificata, essi dovranno essere inviati all'indirizzo di posta elettronica istituzionale non certificata. La casella di posta elettronica non certificata di settore, ufficio o personale va utilizzata dalle strutture per tutte le comunicazioni aventi solamente carattere informale (come precisato nella circolare n. 1/ 2010/ DDI del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica) e per le comunicazioni aventi natura non ufficiale o per gli scambi di documenti non definitivi e per i quali non è comunque necessario acquisire certezza di invio e di ricezione, sia fra le strutture dell'Ente che fra queste ultime e altre amministrazioni. Pertanto, le comunicazioni suddette, saranno trasmesse esclusivamente con le caselle di posta elettronica non certificata di settore, ufficio o personale. In caso di ricezione nella casella di posta elettronica degli uffici di documenti da protocollare, questi dovranno essere inoltrati all'indirizzo di posta elettronica istituzionale non certificata associata al registro di protocollo informatico.

#### *5.10 Produzione di copie e duplicati*

Il Codice dell'Amministrazione Digitale, Decreto Legislativo n. 82 del 2005 e sue successive modificazioni, definisce così le varie possibilità di copie di documenti:

i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento da cui è tratto;

i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinques) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

Le copie per immagine di originali analogici hanno valore legale inferiore all'originale da cui sono tratti se un pubblico ufficiale a ciò autorizzato non attesta la copia di conformità con apposita formula e firma.

Le copie analogiche di originali digitali hanno lo stesso valore legale dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale.

Di seguito vengono riportate alcune frasi di riferimento per poter procedere alle copie conformi:

COMUNE DI SANTA GIUSTINA IN COLLE

ATTESTAZIONE DI COPIA CONFORME ANALOGICA DA ORIGINALE DIGITALE

Io sottoscritto/a \_\_\_\_\_ in qualità di \_\_\_\_ dell'Ufficio \_\_\_\_\_ attesto con firma autografa che il presente atto ai sensi dell'art 23 del d. lgs 82 del 2005 costituisce copia conforme analogica di documento originale digitale conservato a raccolta a cura di questo Comune di SANTA GIUSTINA IN COLLE.

SANTA GIUSTINA IN COLLE : \_\_\_\_\_

Il funzionario incaricato

Nome e cognome

COMUNE DI SANTA GIUSTINA IN COLLE

ATTESTAZIONE DI COPIA CONFORME INFORMATICA DA ORIGINALE ANALOGICO

Io sottoscritto/a \_\_\_\_\_ in qualità di \_\_\_\_ dell'Ufficio \_\_\_\_\_ attesto con firma digitale che il presente atto ai sensi dell'art 22 del d.lgs 82 del 2005 costituisce copia conforme informatica di documento originale analogico conservato a raccolta presso questo Comune di SANTA GIUSTINA IN COLLE.

SANTA GIUSTINA IN COLLE : \_\_\_\_\_

Il funzionario incaricato

Nome e cognome

COMUNE DI SANTA GIUSTINA IN COLLE

ATTESTAZIONE DI COPIA CONFORME INFORMATICA DI ORIGINALE INFORMATICO

Io sottoscritto/a \_\_\_\_\_ in qualità di \_\_\_\_ dell'Ufficio \_\_\_\_\_ attesto con firma digitale che il presente atto ai sensi dell'art 23 bis del d. lgs 82 del 2005 costituisce copia conforme digitale di originale digitale conservato a raccolta a cura di questo Comune di SANTA GIUSTINA IN COLLE.

SANTA GIUSTINA IN COLLE : \_\_\_\_\_

Il funzionario incaricato

Nome e cognome

#### **NOTA BENE SU QUESTA ATTESTAZIONE DI COPIE INFORMATICHE DI ORIGINALE INFORMATICO**

Questa formula sopra esposta di attestazione è da utilizzare quando tra copia e originale avviene un cambiamento della sequenza dei valori binari che costituiscono il file. (esempio da un word ad un pdf oppure da excel a pdf).

**Non necessitano invece di alcuna formula di conformità i duplicati informatici.**

Secondo il CAD D.Lgs 82/2005 (art. 1 definizioni) il duplicato informatico è il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Esempio: un contratto nativo digitale, che è un pdf.p7m, va inviato al contraente mantenendolo in ambiente digitale senza necessità di fare copia conforme, in quanto si è di fronte ad un duplicato.

**Dunque i documenti nativi digitali, se non vengono modificati, non necessitano di attestazione di copia conforme perché sono duplicati e non copie.**

Questo concetto viene ribadito nell'art. 5 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 novembre 2014 **Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni** ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

Di seguito vengono riportate alcune frasi di riferimento specifiche per il servizio di stato civile (trasmissione informatica degli atti cartacei da trascrivere) :

COMUNE DI SANTA GIUSTINA IN COLLE (PD)

UFFICIO DELLO STATO CIVILE

Si certifica la conformità del presente documento all'atto cartaceo originale ai sensi della Circolare del Ministero dell'Interno n. 14 del 18/5/2011, per uso trascrizione nel Comune di Santa Giustina in Colle (art. 12 D.P.R. 3/11/2000, n. 396).

Santa Giustina in Colle, li \_\_\_\_\_

L'Ufficiale di Stato Civile

### *5.11 Trasmissioni telematiche*

I dati trasmessi dall'Ente con immissione diretta dei dati sul server ministeriale/ente destinatario, mediante interfaccia web, senza la produzione e conservazione dell'originale cartaceo, non vanno protocollati, salvo richiesta particolare dell'ente destinatario. I documenti sono trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca attivati con i singoli Enti destinatari.

Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

## SEZIONE VI. ASSEGNAZIONE DEI DOCUMENTI

### *6.1 Assegnazione e consegna*

L'assegnazione dei documenti agli uffici utenti o ai responsabili di procedimento per competenza/conoscenza è effettuata sulla base dell'organigramma dell'Amministrazione. I documenti ricevuti dall'Ente, al termine delle operazioni di registrazione, classificazione, segnatura ed assegnazione, sono fatti pervenire agli uffici che, per quanto a conoscenza dell'ufficio protocollo, hanno competenza sull'oggetto specificato nel documento. I documenti ricevuti in forma analogica, anche se successivamente acquisiti in formato immagine, sono assegnati agli uffici con la registrazione di protocollo e resi disponibili ai destinatari mediante l'uso di apposite cassette. I documenti informatici sono assegnati agli uffici con la registrazione di protocollo e resi disponibili ai destinatari tramite la procedura informatica di gestione protocollo e gestione documentale. Spettano al responsabile del procedimento amministrativo le incombenze relative alla gestione del documento: l'inserimento nel fascicolo di competenza preesistente o eventualmente in un nuovo fascicolo.

### *6.2 Modifica delle assegnazioni*

Nel caso di un'assegnazione errata, l'ufficio che riceve il documento, lo rinvia o comunica all'ufficio Protocollo, che provvederà alla riassegnazione per poi trasmetterlo al nuovo assegnatario. La responsabilità del mancato rispetto di quanto sopra descritto è da attribuirsi all'Ufficio che non ha rimandato al servizio Protocollo il documento erroneamente trasmesso.

Delle operazioni di riassegnazione è lasciata traccia nel sistema informatico di gestione dei documenti.

In caso di documentazione informatica, il software di gestione documentale provvederà automaticamente a rendere visibile il documento riassegnato al destinatario di competenza.

Il sistema informatico di Protocollo tiene traccia di tutti i passaggi, memorizzando per ciascuno di essi l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.



## SEZIONE VII. CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

### *7.1 Classificazione dei documenti*

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario. I documenti in arrivo sono classificati dall'ufficio protocollo. I documenti prodotti dall'Ente sono classificati e protocollati da chi li scrive.

Fino al 31/12/2015 è utilizzato il Titolario di cui alla Circolare Astengo. Dal 01/01/2016 è adottato il nuovo Titolario, approvato con deliberazione della Giunta Comunale n. 99 del 21/09/2015 (allegato 6).

I documenti interni, che pur non rivestendo un carattere giuridico-probatorio tale da comportare la necessità di registrazione a protocollo, rivestono importanza quale testimonianza dei processi decisionali e dell'attività complessiva dell'ente, possono comunque essere classificati e fascicolati, affinché rimanga traccia anche dell'attività interlocutoria e conoscitiva dell'ente in tutte le sue fasi. La classificazione e la fascicolazione sono effettuate da ogni singolo Responsabile di procedimento.

### *7.2 Formazione e identificazione dei fascicoli*

Tutti i documenti registrati al Protocollo Informatico e classificati, indipendentemente dal supporto sul quale sono forniti, devono essere riuniti in fascicoli.

Il fascicolo è l'insieme ordinato di documenti, relativi a uno stesso affare/procedimento/processo amministrativo, a una stessa materia, a una stessa tipologia, che si forma sempre nel corso delle attività amministrative del soggetto, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo sono generalmente inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se non è infrequente la creazione di fascicoli formati da insiemi di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, per materia ecc.). I fascicoli costituiscono la componente più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri diversi che sono, tuttavia, stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento. Nei casi in cui insorgano esigenze pratiche, il fascicolo può essere distinto in sottofascicoli e questi in pratiche.

Mediante la classificazione si assegna al documento il Titolo e la Classe, eventualmente il numero del fascicolo ed eventualmente del sottofascicolo.

La classificazione dei documenti inviati, ricevuti ed interni formali, viene, di norma, effettuata dagli addetti degli Uffici competenti.

### *7.3 Processo di formazione dei fascicoli*

In presenza di un documento da inserire in un fascicolo i responsabili di servizio/ procedimento stabiliscono, consultando le funzioni del protocollo informatico o il repertorio dei fascicoli, se esso si collochi nell'ambito di un affare o procedimento in corso, oppure se dà avvio ad un nuovo procedimento.

I documenti sono fascicolati dai responsabili di procedimento, che hanno cura di inserirli fisicamente nel fascicolo, in caso di documenti cartacei; nel caso di documenti informatici, il sistema di protocollo informatico e gestione documentale consente la formazione dei fascicoli informatici.

### *7.5 Fascicolo ibrido*

Il fascicolo è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema mediante l'indice di classificazione e il numero di repertorio. Vedi anche articoli 9.1 e 9.2.

Alla chiusura del fascicolo, ai sensi del Codice dell'Amministrazione digitale (D. Lgs. n. 82/ 2005) sono previste due possibilità:

- 1) stampa e copia conforme cartacea dell'originale informatico;
- 2) scansione e copia conforme informatica dell'originale cartaceo.

Il Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi" mantiene comunque un'attività di controllo sulle procedure suddette.

Il documento originale sarà conservato secondo quanto previsto dal massimario di scarto (Allegato n. 10).

I documenti originali informatici saranno sottoposti al procedimento di conservazione sostitutiva. I documenti originali cartacei saranno inviati in archivio di deposito in apposite scatole o faldoni contenenti l'indicazione della classificazione e dell'anno di produzione/ ricevimento.

### *7.6 Archivio corrente e di deposito*

Il sistema archivistico è unico all'interno della AOO anche se, funzionalmente è strutturato in una sezione corrente, una di deposito e storica.

La sezione corrente è, di norma, gestita dai Responsabili dei Procedimenti Amministrativi in quanto trattasi di documenti in corso di lavorazione, ovvero di documenti relativi ad affari o procedimenti non ancora conclusi.

La sezione corrente viene alimentata dalla corrispondenza ricevuta, inviata e/o interna formale relativa ad uno stesso affare conservata all'interno dei fascicoli elettronici/cartacei.

L'archivio attualmente presenta una gestione mista (supporto cartaceo e informatico), data dalla natura stessa degli originali.

Gli archivi e i singoli documenti degli enti pubblici sono considerati beni culturali, assoggettati al regime proprio del demanio pubblico.

I singoli documenti (analogici ed informatici, ricevuti, spediti e interni formali) e l'archivio dell'Amministrazione nel complesso sono quindi beni culturali appartenenti al demanio pubblico, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'Amministrazione mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

In quanto appartenenti al demanio pubblico gli archivi e i singoli documenti dell'Amministrazione sono inalienabili.

Essi sono conservati nella loro organicità.

Lo scarto di documenti è subordinato all'autorizzazione degli organismi competenti, (Soprintendenza Archivistica della Regione Veneto).

L'archivio è la raccolta ordinata degli atti spediti o ricevuti o interni formali dell'Amministrazione per il conseguimento dei propri fini o l'espletamento delle proprie funzioni e conservati per il conseguimento degli scopi politici giuridici e culturali dell'Amministrazione stessa.

Gli atti sono documenti collegati tra loro con rapporto di causa effetto, sono ordinati ovvero strutturati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico.

Convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio si suddivide in tre sezioni:

a. corrente, costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;

b. di deposito, costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;

c. storico, costituito complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne. L'archivio, pur suddiviso come sopra illustrato, è unico. Tutte le sezioni d'archivio si trovano presso il Municipio e parte piano terra e primo piano dell'edificio pubblico in Piazza San Giacomo, frazione Fratte.

Periodicamente - di norma una volta all'anno e comunque compatibilmente con gli spazi a disposizione - il Responsabile del Procedimento Amministrativo è tenuto a conferire i fascicoli relativi ad affari e a procedimenti amministrativi conclusi o comunque non più necessari ad una trattazione corrente. I fascicoli devono giungere all'archivio di deposito in ordine e senza carte superflue, con la chiara indicazione del loro contenuto scritto in sintesi sulla costola del faldone o sulla copertina del fascicolo.

La regolare periodicità dell'operazione è fondamentale per garantire la qualità del materiale depositato.

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

Prima di effettuare il conferimento di cui sopra, il Responsabile del Procedimento Amministrativo procede alla verifica:

dell'effettiva conclusione ordinaria della pratica;

del corretto aggiornamento della data di chiusura sulla copertina del fascicolo ed alla eliminazione di eventuali fotocopie di documentazione istruttoria al fine di garantire la presenza di tutti e soli i documenti formali pertinenti alla pratica in oggetto;

che il materiale pronto per essere riversato sia correttamente organizzato e corredato da informazioni relative alla pratica che ne garantiscano l'identificazione.

I fascicoli relativi al personale dipendente vanno versati di norma dall'archivio corrente all'archivio di deposito alla definizione della pratica pensionistica.

Le norme sono valide sia per i flussi di documenti cartacei che per quelli informatici.

Per l'archiviazione e la custodia dei documenti contenenti dati personali o comunque riservati, si applicano, in ogni caso, le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

Periodicamente, sulla base dei termini stabiliti dal "MASSIMARIO DI SELEZIONE E SCARTO", sono effettuate le operazioni di selezione e scarto dei fascicoli dall'archivio di deposito. La selezione è l'operazione con la quale vengono individuate le unità archivistiche da avviare allo scarto. Quelle che invece sono da conservare saranno successivamente destinate a far parte dell'archivio storico.

Lo scarto di documenti è sempre subordinato ad autorizzazione della Soprintendenza Archivistica territorialmente competente.

I documenti destinati a far parte della sezione storica dell'archivio vengono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

La richiesta di consultazione, e di conseguenza di movimentazione dei fascicoli, può pervenire dall'interno dell'Amministrazione/AOO o dall'esterno da parte di studiosi e ricercatori, che dovranno compilare l'apposito modulo (**Allegato 7**).

La richiesta di consultazione ai fini di ricerca scientifica è disciplinata dalla gratuità e libertà della ricerca.

a. L'accesso all'archivio di deposito e storico è consentito previa autorizzazione del Responsabile degli Archivi.

b. La consultazione dei documenti da parte di personale esterno all'Amministrazione è possibile esclusivamente in un locale appositamente predisposto sotto la diretta sorveglianza del personale addetto al Protocollo.

c. Il rilascio di copie dei documenti dell'archivio avviene previo pagamento delle sole spese di riproduzione.

d. In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile ne dà comunicazione.

## SEZIONE VIII. SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO

### *8.1 Spedizione dei documenti analogici*

I documenti da spedire sono trasmessi all'ufficio spedizione completi del numero di protocollo. Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate e autorizzate dal Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi".

### *8.2 Spedizione dei documenti informatici*

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti con le procedure adottate dal manuale operativo dello stesso (Allegato n. 9), dopo essere stati classificati, fascicolati e protocollati e comunque secondo i seguenti criteri generali:

- 1) i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via elettronica, tramite casella di posta elettronica certificata;
- 2) quando prescritta, la sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale conforme alle disposizioni contenute nel testo unico e alle regole tecniche dettate dalla vigente normativa.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del CAD D. Lgs. 82/ 05 come modificato dal D. Lgs. 235/ 10.

Per l'uso della posta elettronica si rimanda all'articolo n. 5.9. La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'amministrazione riconosca un carattere giuridico - amministrativo che la impegni verso terzi.

## SEZIONE IX. SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

### *9.1 Documenti soggetti a scansione*

I documenti su supporto cartaceo, di formato inferiore o uguale all'A4, dopo le operazioni di registrazione, classificazione e segnatura, possono essere acquisiti in formato immagine con l'ausilio di scanner.

I documenti ricevuti dall'esterno su formato cartaceo sono registrati al protocollo generale e classificati e successivamente scansionati; successivamente alla scansione, la copia immagine del documento è resa disponibile sulla postazione di lavoro dell'UO unitamente alla copia cartacea dello stesso.

### *9.2 Processo di scansione*

Il processo di scansione si articolerà di massima nelle seguenti fasi:

- 1) acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard abilitato alla conservazione (PDF – PDF/ A TIFF - JPG);
- 2) verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- 3) collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- 4) memorizzazione delle immagini, in modo non modificabile.

## SEZIONE X. CONSERVAZIONE E TENUTA DEI DOCUMENTI

### *10.1 Conservazione dei documenti informatici*

La documentazione corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

La documentazione trasferita in archivio di deposito è conservata a cura del servizio Protocollo.

A far data dal 12/10/2015 il registro giornaliero di protocollo del Comune di Santa Giustina in Colle è conservato a cura del Responsabile della Conservazione (vedi articolo n. 1.4 e Allegato 21) in modo conforme a quanto previsto dal D.P.C.M 3 dicembre 2013 – *Regole tecniche in materia di sistema di conservazione*, dal D. M.E.F. del 17 giugno 2014, dal D.P.R. 633/ 72, dalla Circolare dell’Agenzia delle Entrate n. 45/ E del 19 ottobre 2005, dalla Circolare dell’Agenzia delle Entrate n. 36/ E del 6 dicembre 2006 e loro successive modificazioni o integrazioni, come specificato nel Manuale della Conservazione (Allegato n. 8).

### *10.2 Selezione e conservazione dei documenti*

Ogni anno, in base al massimario di scarto e compatibilmente con le esigenze di servizio, viene effettuata la procedura di selezione della documentazione da proporre allo scarto e attivato il procedimento amministrativo di scarto documentale con l’invio della proposta alla competente Soprintendenza archivistica. I fascicoli non soggetti a operazioni di scarto sono trasferiti nell’archivio storico per la conservazione permanente, sia essa analogica o digitale. Il Manuale di gestione e i relativi aggiornamenti devono essere conservati integralmente e perennemente nell’archivio dell’Ente.

## SEZIONE XI. PIANO DI SICUREZZA

### *11.1 Obiettivi del Piano di sicurezza*

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal Comune di Santa Giustina in Colle 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.

### *11.2 Formazione dei documenti informatici – aspetti di sicurezza*

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

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

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale o avanzata, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, come riportato sul sito dell'Agenzia per l'Italia Digitale ([www.agid.gov.it](http://www.agid.gov.it)), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. A titolo d'esempio si utilizzano preferibilmente: PDF e PDF/ A.

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

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) presenti o transitate nel sistema di Protocollo Informatico che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.



#### *11.4 Accesso ai documenti informatici*

La profilazione degli utenti avviene in via preventiva e consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate a ogni singolo utente.

Il sistema di protocollo informatico adottato dal Comune di Santa Giustina in Colle:

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

Ciascun utente del Protocollo Informatico può accedere solamente ai documenti che sono stati direttamente assegnati. Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'Amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

#### *11.5 Utenti interni alla AOO*

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti con il permesso del Responsabile del "Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi". Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

#### *11.6 Profili utente e responsabilità*

Il sistema garantisce la tutela dei dati personali e dei dati sensibili tramite l'assegnazione differenziata dei diritti di modifica e di visualizzazione dei documenti di protocollo in rapporto alle funzioni e al ruolo svolto dagli utenti.

Il sistema prevede diverse possibilità di combinazione dei profili di accesso al protocollo informatico:

- visibilità: possibilità per un utente abilitato di visualizzare una registrazione di protocollo, con l'esclusione dei documenti riservati;
- inserimento: possibilità per un utente abilitato di inserire i dati e provvedere ad una registrazione di protocollo;
- modifica: possibilità per un utente abilitato di modificare i dati gestionali di una registrazione di protocollo, con l'esclusione dei dati obbligatori;
- annullamento: possibilità per un utente abilitato di annullare una registrazione di protocollo.

### *11.7 Conservazione dei documenti informatici*

La conservazione dei documenti informatici avviene a cura del Responsabile della Conservazione (Allegato 8) in modo conforme a quanto previsto dal D.P.C.M. 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione, dal D. M.E.F. del 17 giugno 2014, dal D.P.R. 633/ 72, dalla Circolare dell’Agenzia delle Entrate n. 45/ E del 19 ottobre 2005, dalla Circolare dell’Agenzia delle Entrate n. 36/ E del 6 dicembre 2006 e loro successive modificazioni o integrazioni, come specificato nel Manuale della Conservazione (Allegato n. 8) e nella Sezione X.

## SEZIONE XII. ACCESSO

### *12.1 Accessibilità da parte degli utenti appartenenti all'Amministrazione*

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password, o altre tecniche e dispositivi di autenticazione sicura.

L'Amministrazione, in conformità alla normativa vigente, assicura il diritto di accesso ai documenti riguardanti il procedimento amministrativo da parte di utenti esterni, garantendo la tutela alla riservatezza.

I documenti conservati nell'Archivio sono liberamente consultabili per il combinato disposto degli art. 58 – 59 – 60 del Testo Unico, fatte salve le norme vigenti sul segreto e sulla tutela della riservatezza.

### *12.2 Accesso esterno*

L'accesso al sistema informatico da parte di utenti esterni può avvenire solo con l'impiego di sistemi di riconoscimento e autenticazione sicuri basati su certificato digitale secondo quanto previsto dall'articolo 65 del Decreto Legislativo 7 marzo 2005, n. 82 e, nei casi di particolari procedimenti amministrativi con credenziali di accesso rilasciate dall'Ente.

## SEZIONE XIII. APPROVAZIONE, REVISIONE E PUBBLICAZIONE

### *13.1 Approvazione*

Il presente Manuale è adottato dall'Amministrazione con proprio provvedimento, su proposta del Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi”,

### *13.2 Revisione*

Il presente Manuale è rivisto, ordinariamente, ogni due anni su iniziativa del Responsabile del “Servizio per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi”. Qualora se ne presenti la necessità, si potrà procedere a revisione o integrazione del manuale anche prima della scadenza prevista.

### *13.3 Pubblicazione*

Il Manuale di Gestione è reso pubblico tramite la sua diffusione sul sito web dell'Amministrazione [www.comunesgcolle.gov.it](http://www.comunesgcolle.gov.it)

## ALLEGATI:

- Allegato 1) Individuazione A.O.O. e nomina Responsabile della gestione documentale (deliberazione della G.C. n. 92/2015)
- Allegato 2) Glossario e formati (allegato al DPCM 3 dicembre 2013)
- Allegato 3) Elenco dei repertori (approvato con deliberazione della G.C. n. 99/2015)
- Allegato 4) Elenco delle Unità organizzative dell'Ente ed elenco uffici con abilitazione alla protocollazione
- Allegato 5) Protocollo di emergenza – breve guida per l'attivazione
  - 5.1 Autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza
  - 5.2 Protocollo di emergenza
  - 5.3 Revoca autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza
- Allegato 6) Titolare Astengo (utilizzato fino al 31.12.2015) e Titolare utilizzato dal 01.01.2016 (approvato con deliberazione della G.C. n. 99/2015)
- Allegato 7) Modulo richiesta accesso all'archivio storico
- Allegato 8) Manuale dei processi di formazione e conservazione dei documenti elettronici (approvato con deliberazione della G.C. n. 102/2015)
- Allegato 9) Manuale di utilizzo “Protocollo e Atti”



# COMUNE DI S. GIUSTINA IN COLLE

PROVINCIA DI PADOVA

## Verbale di Deliberazione della Giunta Comunale

Oggetto: Individuazione AOO e nomina Responsabile della gestione documentale				
L'anno <b>duemilaquindici</b> addì <b>sette</b> del mese di <b>settembre</b> alle ore <b>19.00</b> nella Residenza Municipale, per determinazione del Sindaco, si e' riunita la Giunta Comunale.				
<input type="checkbox"/> Soggetta invio Capigruppo Consiliari	Risultano presenti alla trattazione dell'argomento in oggetto:		<b>Presenti</b>	<b>Assenti</b>
	1. Gallo Paolo	Sindaco	X	
	2. Ruffato Gianluca	Assessore Effettivo	X	
	3. Cagnin Raffaella	Assessore Effettivo	X	
	4. Giason Paolo	Assessore Effettivo	X	
	5. Mengato Franca	Assessore Effettivo	X	
	6.			
	7.			
Partecipa alla seduta il Segretario Comunale Sig. Pontini Claudio.				
Il Sig. Gallo Paolo nella sua qualita' di Sindaco assume la presidenza e, riconosciuta legale l'adunanza, dichiara aperta la seduta.				

Reg.n° \_\_\_\_\_

### REFERTO DI PUBBLICAZIONE

(art. 124 D.Lgs. 18/08/2000, n.267)

Il sottoscritto Segretario Comunale, su conforme dichiarazione del Messo Comunale, attesta che copia del presente verbale viene affisso all'Albo Pretorio, dove restera' per 15 gg. consecutivi dal \_\_\_\_\_ al \_\_\_\_\_.

E' stata comunicata, con lettera n. \_\_\_\_\_, in data \_\_\_\_\_, ai Capigruppo consiliari cosi' come prescritto dall'art.125 del D.Lgs. 18.08.2000, n.267.

li',

Il Segretario Comunale  
Fto Pontini Claudio

## LA GIUNTA COMUNALE

**VISTO** l'art. 3 D.P.C.M. 3 dicembre 2013 che prevede di istituire all'interno di ogni Pubblica Amministrazione le aree organizzative omogenee e gli uffici di riferimento nonché di nominare il Responsabile della gestione documentale;

**CONSIDERATO** che si intende per Area Organizzativa Omogenea (AOO) un insieme di funzioni e strutture, individuate dall'Amministrazione, che operano su tematiche omogenee e che presentano esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'art. 2 comma 2 del DPR 428/ 1998;

**VISTO** il D.P.R. 445/ 2000 "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*" che prevede all'art. 50 che tutte le Pubbliche Amministrazioni individuino nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi AOO, assicurando criteri uniformi di classificazione e archiviazione;

**RITENUTO** di procedere all'individuazione e alla definizione all'interno dell'Amministrazione Comunale di Santa Giustina in Colle di un'unica AOO, ai fini di avere un'unica gestione dei documenti;

**VISTO**, altresì, l'art. 61 del D.P.R. 445/ 2000, il quale dispone che ogni Amministrazione istituisca un Servizio per la tenuta del protocollo informatico, della gestione di flussi documentali e degli archivi in ciascuna delle AOO individuate ai sensi del sopracitato art. 50, e che questo sia posto alle dirette dipendenze della suddetta AOO, e che dispone, inoltre, che al Servizio siano preposti un Responsabile ed un suo Vicario per casi di assenza o impedimento del primo;

**CONSIDERATO** che per il Comune di Santa Giustina in Colle il Servizio di Segreteria e Protocollo è affidato al Responsabile del 1° Settore "Economico-Finanziario-Affari Generali" e che il protocollo informatico è utilizzato dagli uffici comunali dal 2/2/2004 mediante software informatico fornito dalla ditta Kibernetes srl di Silea (TV) e denominato "Protocollo e Atti";

**CONSIDERATO** che obiettivo fondamentale rimane anche quello di migliorare la trasparenza dell'azione amministrativa attraverso strumenti che consentano l'accesso allo stato dei procedimenti e ai relativi documenti da parte di cittadini, imprese ed altre Amministrazioni;

**VISTO** il D. Lgs. 267/ 2000 e s.m.i.;

**VISTI** i pareri resi, in allegato al presente provvedimento, ai sensi degli articoli 49 e 147-bis del D. Lgs. n. 267/2000, e successive modifiche ed integrazioni;

**DATO ATTO** che, in ordine alla presente proposta di deliberazione, il Segretario Generale non ha sollevato alcun rilievo in ordine alla conformità alle leggi, allo statuto e ai regolamenti, ai sensi dell'art. 97, comma 2° del D.Lgs. 18 agosto 2000, n. 267;

Con voti favorevoli unanimi legalmente espressi,

### DELIBERA

1) DI INDIVIDUARE per i motivi espressi in premessa una sola AOO nell'ambito dell'Amministrazione Comunale di Santa Giustina in Colle;

2) DI ISTITUIRE il Servizio per la tenuta del protocollo informatico, della gestione di flussi documentali e degli archivi individuato funzionalmente nell'ambito del 1° Settore "Economico-Finanziario-Affari Generali", precisando che a tale servizio sono ricondotti i compiti di cui all'art. 61 comma 3 del D.P.R. 445/ 2000;

3) DI INDIVIDUARE, pertanto, ai sensi dell'art. 61 del D.P.R. 445/ 2000 e s.m.i., quale Responsabile del Servizio per la tenuta del protocollo informatico, della gestione di flussi documentali e degli archivi il Responsabile del Settore Economico-Finanziario-Affari Generali;

4) DI INDIVIDUARE quale Vicario in caso di assenza o impedimento del Responsabile del 1° Settore il dipendente di categoria più elevata inquadrato nel medesimo Settore;

5) DI DICHIARARE la presente Deliberazione immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D. Lgs n. 267/ 2000.

## PARERI

Regolarità tecnica: (art. 49 comma 1° del D.Lgs. n. 267/2000)

Favorevole

Il Responsabile del Servizio

Fto Fiorenza Verzotto

---

Regolarità contabile: (artt. 49 comma 1° e 151 comma 4 del D.Lgs. n. 267/2000)

Parere non dovuto

Il Ragioniere Capo

Fto Fiorenza Verzotto

---



Il presente verbale viene letto e sottoscritto come segue:

---

**IL PRESIDENTE**  
FtoGallo Paolo

**IL SEGRETARIO COMUNALE**  
Fto Pontini Claudio

---

**Copia conforme all'originale in carta libera per uso amministrativo.**

Li, .....

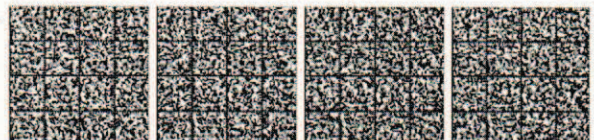
**IL SEGRETARIO COMUNALE**  
F.to Pontini Claudio

## GLOSSARIO/DEFINIZIONI

### Indice

- 1 INTRODUZIONE
- 2 DEFINIZIONI

*Allegato alle Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici*

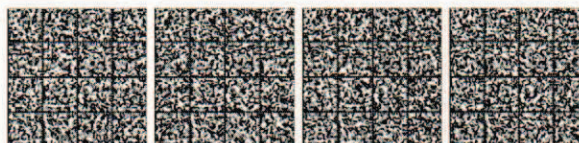


## 1 INTRODUZIONE

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizioni del citato decreto ed a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

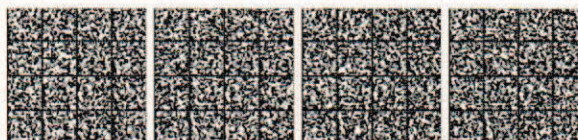
## 2 DEFINIZIONI

TERMINE	DEFINIZIONE
<b>accesso</b>	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
<b>accreditamento</b>	riconoscimento, da parte dell' <b>Agenzia per l'Italia digitale</b> , del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
<b>affidabilità</b>	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
<b>aggregazione documentale informatica</b>	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
<b>archivio</b>	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
<b>archivio informatico</b>	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
<b>area organizzativa omogenea</b>	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
<b>attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
<b>autenticità</b>	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
<b>base di dati</b>	collezione di dati registrati e correlati tra loro



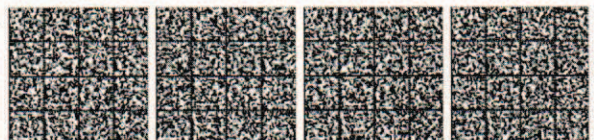


TERMINE	DEFINIZIONE
<b>certificatore accreditato</b>	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, <b>dall' Agenzia per l'Italia digitale</b> , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
<b>ciclo di gestione</b>	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
<b>classificazione</b>	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
<b>Codice</b>	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
<b>codice eseguibile</b>	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
<b>conservatore accreditato</b>	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, <b>dall'Agenzia per l'Italia digitale</b> , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, <b>dall'Agenzia per l'Italia digitale</b>
<b>conservazione</b>	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
<b>Coordinatore della Gestione Documentale</b>	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
<b>copia analogica del documento informatico</b>	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
<b>copia di sicurezza</b>	copia di <i>backup</i> degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
<b>destinatario</b>	identifica il soggetto/sistema al quale il documento informatico è indirizzato
<b>duplicazione dei documenti informatici</b>	produzione di duplicati informatici
<b>esibizione</b>	operazione che consente di visualizzare un documento conservato e di ottenerne copia
<b>estratto per riassunto</b>	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
<b>evidenza informatica</b>	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
<b>fascicolo informatico</b>	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.



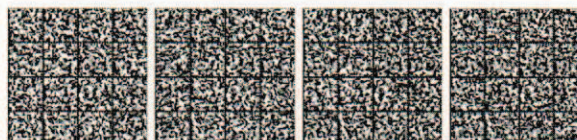


TERMINE	DEFINIZIONE
<b>formato</b>	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
<b>funzionalità aggiuntive</b>	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
<b>funzionalità interoperative</b>	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
<b>funzionalità minima</b>	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
<b>funzione di hash</b>	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
<b>generazione automatica di documento informatico</b>	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
<b>identificativo univoco</b>	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
<b>immodificabilità</b>	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
<b>impronta</b>	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
<b>insieme minimo di metadati del documento informatico</b>	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
<b>integrità</b>	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
<b>interoperabilità</b>	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
<b>leggibilità</b>	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
<b>log di sistema</b>	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
<b>manuale di conservazione</b>	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione



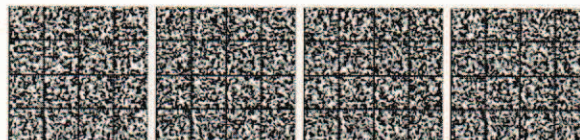


TERMINE	DEFINIZIONE
<b>manuale di gestione</b>	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
<b>memorizzazione</b>	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
<b>metadati</b>	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto
<b>pacchetto di archiviazione</b>	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
<b>pacchetto di distribuzione</b>	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
<b>pacchetto di versamento</b>	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
<b>pacchetto informativo</b>	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
<b>piano della sicurezza del sistema di conservazione</b>	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
<b>piano della sicurezza del sistema di gestione informatica dei documenti</b>	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
<b>piano di conservazione</b>	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
<b>piano generale della sicurezza</b>	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
<b>presa in carico</b>	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
<b>processo di conservazione</b>	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione



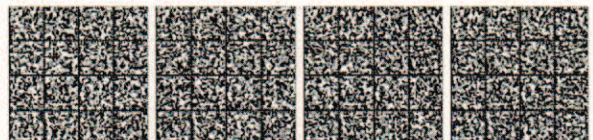


TERMINE	DEFINIZIONE
<b>produttore</b>	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
<b>rapporto di versamento</b>	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
<b>registrazione informatica</b>	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
<b>registro particolare</b>	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
<b>registro di protocollo</b>	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
<b>repertorio informatico</b>	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
<b>responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi</b>	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
<b>responsabile della conservazione</b>	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
<b>responsabile del trattamento dei dati</b>	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
<b>responsabile della sicurezza</b>	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
<b>riferimento temporale</b>	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
<b>scarto</b>	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
<b>sistema di classificazione</b>	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata





TERMINE	DEFINIZIONE
<b>sistema di conservazione</b>	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
<b>sistema di gestione informatica dei documenti</b>	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
<b>staticità</b>	Caratteristica che garantisce 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
<b>transazione informatica</b>	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
<b>Testo unico</b>	decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
<b>ufficio utente</b>	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
<b>utente</b>	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
<b>versamento agli archivi di stato</b>	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali





# FORMATI

## Indice

- 1 INTRODUZIONE
- 2 I FORMATI
  - 2.1 Identificazione
  - 2.2 Le tipologie di formato
  - 2.3 Formati Immagini
    - 2.3.1 Raster
    - 2.3.2 Vettoriale
  - 2.4 Altri Formati
  - 2.5 Le caratteristiche generali dei formati
- 3 CRITERI DI SCELTA DEI FORMATI
  - 3.1 Caratteristiche
    - 3.1.1 Apertura
    - 3.1.2 Sicurezza
    - 3.1.3 Portabilità
    - 3.1.4 Funzionalità
    - 3.1.5 Supporto allo sviluppo
    - 3.1.6 Diffusione
- 4 SCELTA
  - 4.1 Formati e prodotti per la formazione e gestione
  - 4.2 Formati per la conservazione
- 5 I FORMATI INDICATI PER LA CONSERVAZIONE
  - 5.1 PDF - PDF/A
  - 5.2 TIFF
  - 5.3 JPG
  - 5.4 Office Open XML (OOXML)
  - 5.5 Open Document Format
  - 5.6 XML
  - 5.7 TXT
  - 5.8 Formati Messaggi di posta elettronica



## 1 Introduzione

Il presente documento fornisce indicazioni iniziali sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.

I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.

Il presente documento, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e pubblicato online sul sito dell'Agenzia per l'Italia digitale.

## 2 I formati

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

### 2.1 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].docx identifica un formato testo di proprietà della Microsoft;
2. I metadati espliciti: l'indicazione "application/msword" inserita nei tipi MIME che indica un file testo realizzato con l'applicazione Word della Microsoft
3. il **magic number**: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg

### 2.2 Le tipologie di formato

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione.

Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

In particolare, volendo fare una prima sommaria, e non esaustiva, catalogazione dei più diffusi formati, secondo il loro specifico utilizzo possiamo elencare:

- Testi/documenti (DOC, HTML, PDF,...)
- Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)
- Suoni (MP3, WAV, ...)





- Video (MPG, MPEG, AVI, WMV,...)
- Eseguibili (EXE, ...)
- Archiviazione e Compressione (ZIP, RAR, ...)
- Formati email (SMTP/MIME, ...)

## 2.3 Formati Immagini

Per la rappresentazione delle immagini sono disponibili diversi formati, che possono essere distinti secondo la grafica utilizzata: raster o vettoriale.

### 2.3.1 Raster

Nel caso della grafica raster, l'immagine digitale è formata da un insieme di piccole aree uguali (pixel), ordinate secondo linee e colonne.

I formati più diffusi sono il .tif (usato dai fax), il .jpg, il .bmp.

### 2.3.2 Vettoriale

La grafica vettoriale è una tecnica utilizzata per descrivere un'immagine mediante un insieme di primitive geometriche che definiscono punti, linee, curve e poligoni ai quali possono essere attribuiti colori e anche sfumature.

I documenti realizzati attraverso la grafica vettoriale sono quelli utilizzati nella stesura degli elaborati tecnici, ad esempio progetti di edifici.

Attualmente i formati maggiormente in uso sono:

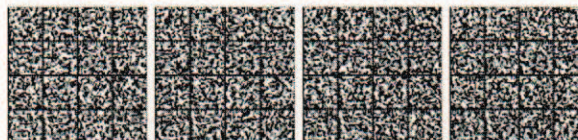
- DWG, un formato proprietario per i file di tipo CAD, di cui non sono state rilasciate le specifiche;
- DXF, un formato simile al DWG, di cui sono state rilasciate le specifiche tecniche
- Shapefile un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con con i prodotti che usano i precedenti formati.
- SVG, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

## 2.4 Altri Formati

Per determinate tipologie di documenti informatici sono utilizzati specifici formati. In particolare in campo sanitario i formati più usati sono:

- DICOM (immagini che arrivano da strumenti diagnostici) anche se il DICOM non è solo un formato, ma definisce anche protocolli e altro;
- HL7 ed in particolare il CDA2 (Clinical Document Architecture) che contiene la sua stessa descrizione o rappresentazione.

Le specifiche approvate per alcune tipologie di documenti quali le prescrizioni, si trovano al seguente indirizzo:





<http://www.innovazionepa.gov.it/i-dipartimenti/digitalizzazione-e-innovazione-tecnologica/attivita/tse/il-tavolo-permanente-per-la-sanita-elettronica-delle-regioni-e-delle-province-autonome-tse-.aspx>

## 2.5 Le caratteristiche generali dei formati

L'informazione digitale è facilmente memorizzata, altrettanto facilmente accedere e riutilizzarla, modificarla e manipolarla, in altre parole, elaborarla ed ottenere nuova informazione.

Questi formati, e i programmi che li gestiscono, che sono poi quelli che consentono e facilitano l'operatività giorno per giorno sul digitale, vanno valutati in funzione di alcune caratteristiche quali:

La diffusione, ossia il numero di persone ed organizzazioni che li adotta

La portabilità, ancor meglio se essa è indotta dall'impiego fedele di standard documentati e accessibili

Le funzionalità che l'utente ha a disposizione per elaborare l'informazione e collegarla ad altre (ad esempio gestione di link)

La capacità di gestire contemporaneamente un numero congruo (in funzione delle esigenze dell'utente) di formati

La diffusione di visualizzatori che consentono una fruibilità delle informazioni in essi contenute indipendentemente dalla possibilità di rielaborarle.

Altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

È facilmente comprensibile come, nella fase di gestione del digitale, l'utente debba avere a disposizione la massima flessibilità possibile in termini di formati e funzionalità disponibili.

Gli unici limiti sono quelli che un'organizzazione impone a se stessa quando per esigenze di interscambio ed interoperabilità, può determinare i formati, e i relativi programmi di gestione, che maggiormente soddisfano le contingenti esigenze operative.

## 3 Criteri di scelta dei formati

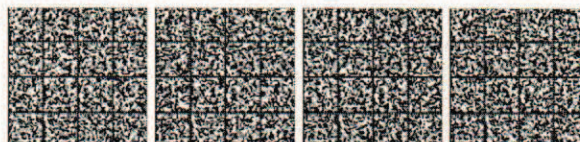
Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono.

### 3.1 Caratteristiche

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura
2. sicurezza
3. portabilità





4. funzionalità
5. supporto allo sviluppo
6. diffusione

### **3.1.1 Apertura**

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.

Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.

Nelle indicazioni di questo documento si è inteso privilegiare i formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e ETSI.

### **3.1.2 Sicurezza**

La sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno

### **3.1.3 Portabilità**

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

### **3.1.4 Funzionalità**

Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

### **3.1.5 Supporto allo sviluppo**

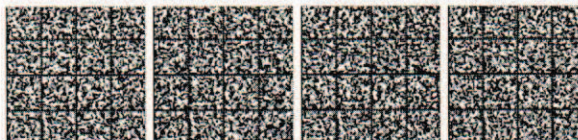
E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

### **3.1.6 Diffusione**

La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici,

Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Inoltre nella scelta dei prodotti Altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.





## 4 Scelta

### 4.1 Formati e prodotti per la formazione e gestione

Per la scelta dei formati idonei alla formazione e gestione dei documenti informatici, sono da tenere in considerazione le caratteristiche indicate nei paragrafi precedenti.

Ulteriori elementi da valutare sono l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento.

Le pubbliche amministrazioni indicano nel manuale di gestione i formati adottati per le diverse tipologie di documenti informatici motivandone le scelte effettuate; **specificano altresì i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.**

### 4.2 Formati per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.

Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti informatici.

Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici.

I formati per la conservazione adottati per le diverse tipologie di documenti informatici devono essere indicati nel manuale di conservazione motivandone le scelte effettuate; sono altresì specificati i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.

## 5 I formati indicati per la conservazione

I formati di seguito indicati sono un primo elenco di formati che possono essere usati per la conservazione.

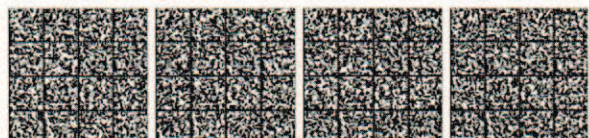
Come già indicato nelle premesse questo elenco sarà periodicamente aggiornato.

### 5.1 PDF - PDF/A

Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. E' stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Nell'attuale versione gestisce varie tipologie di informazioni quali: testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.

Un documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES.

Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.





Sviluppato da	Adobe Systems <a href="http://www.adobe.com/">http://www.adobe.com/</a>
Estensione	.pdf
Tipo MIME	application/pdf
Formato aperto	Si
Specifiche tecniche	Pubbliche
Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
Ultima versione	1.7
Collegamento utile	<a href="http://www.pdfa.org/doku.php">http://www.pdfa.org/doku.php</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.

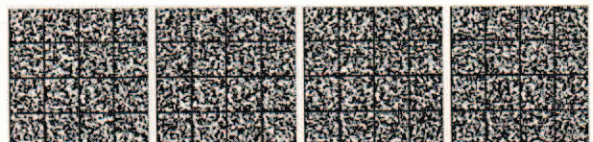
Queste caratteristiche rendono il file indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo.

Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A.

Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.

## 5.2 TIFF

Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
Estensioni	.tif
Tipo MIME	image/tiff
Formato aperto	No
Specifiche tecniche	Pubbliche
Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Collegamenti utili	<a href="http://partners.adobe.com/public/developer/tiff/index.html">http://partners.adobe.com/public/developer/tiff/index.html</a>



Di questo formato immagine raster, in versione non compressa o compressa senza perdita di informazione. Di questo formato vi sono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare). In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione.

Questo è un formato utilizzato per la conversione in digitale di documenti cartacei. Il suo impiego va valutato attentamente in funzione del tipo di documento da conservare in considerazione dei livelli di compressione e relativa perdita dei dati.

Esistono, infine, alcuni formati ISO basati sulla specifica TIFF 6.0 di Adobe (che è quella "ufficiale" del TIFF). Si tratta del formato ISO 12639, altrimenti noto come TIFF/IT, rivolto particolarmente al mondo del publishing e della stampa e dell'ISO 12234, altrimenti detto TIFF/EP, più orientato alla fotografia digitale.

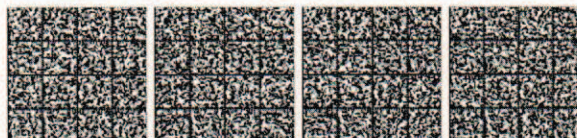
### 5.3 JPG

Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	Si
Specifiche tecniche	Pubbliche
Standard	ISO/IEC 10918:1
Ultima versione	2009
Collegamenti utili	<a href="http://www.jpeg.org/">http://www.jpeg.org/</a> <a href="http://www.iso.org">www.iso.org</a>

Il formato JPEG può comportare una perdita di qualità dell'immagine originale. Anche in questo caso, come nel caso dei TIFF, avendo una grossa diffusione, può essere preso in considerazione, ma il suo impiego, correlato ad un opportuno livello di compressione va valutato attentamente in funzione del tipo di documento da conservare.

JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web.

Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.





#### 5.4 Office Open XML (OOXML)

Sviluppato da	Microsoft <a href="http://www.microsoft.com">http://www.microsoft.com</a> <a href="http://www.microsoft.it">http://www.microsoft.it</a>
Estensioni principali	.docx, .xlsx, .pptx
Tipo MIME	
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da Microsoft dal 2007
Standard	ISO/IEC DIS 29500:2008
Ultima versione	1.1
Possibile presenza codice maligno	Sì
Collegamenti utili	<a href="http://msdn.microsoft.com/en-us/library/aa338205.aspx">http://msdn.microsoft.com/en-us/library/aa338205.aspx</a> <a href="http://standards.iso.org/ittf/PubliclyAvailableStandards">http://standards.iso.org/ittf/PubliclyAvailableStandards</a> <a href="http://www.iso.org">www.iso.org</a>

Comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.

Open XML è adottato dalla versione 2007 della suite Office di Microsoft.

Lo standard prevede, oltre alle indicazioni fondamentali (strict), alcune norme transitorie (transitional) introdotte per ammettere, anche se solo temporaneamente, alcune funzionalità presenti nelle vecchie versioni del formato e la cui rimozione avrebbe potuto danneggiare gli utenti, facendogli perdere funzionalità.

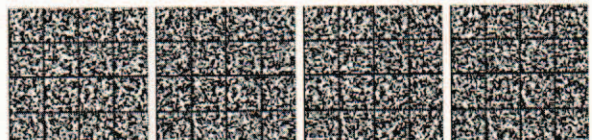
Per quanto riguarda il supporto di Microsoft Office allo standard ISO/IEC 29500:2008:

- MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1.
- MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional e legge file conformi a ISO/IEC 29500:2008 strict

Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato.

Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML.

I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008.



## 5.5 Open Document Format

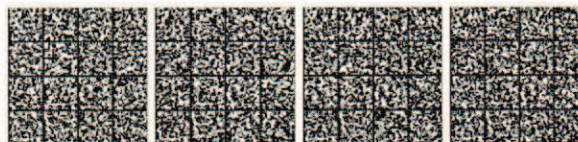
Sviluppato da	OASIS <a href="http://www.oasis-open.org/">http://www.oasis-open.org/</a> Oracle America (già Sun Microsystems) <a href="http://www.oracle.com/it/index.html">http://www.oracle.com/it/index.html</a>
Estensioni	.ods, .odp, .odg, .odb
Tipo MIME	application/vnd.oasis.opendocument.text
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da OASIS dal 2005
Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
Ultima versione	1.0
Collegamenti utili	<a href="http://books.evc-cit.info/">http://books.evc-cit.info/</a> <a href="http://www.oasis-open.org">http://www.oasis-open.org</a>  <a href="http://www.iso.org">www.iso.org</a>

ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni.

Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione.

Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux, Mac.

È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.





## 5.6 XML

Sviluppato da	W3C
Estensioni	.xml
Tipo MIME	application/xml text/xml
Formato aperto	Sì
Specifiche tecniche	pubblicate da W3C <a href="http://www.w3.org/XML/">http://www.w3.org/XML/</a>
Collegamenti utili	<a href="http://www.w3.org/">http://www.w3.org/</a>

Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879).

Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio:

- SVG usato nella descrizione di immagini vettoriali
- XBRL usato nella comunicazione di dati finanziari
- ebXML usato nel commercio elettronico
- SOAP utilizzato nello scambio dei messaggi tra Web Service

## 5.7 TXT

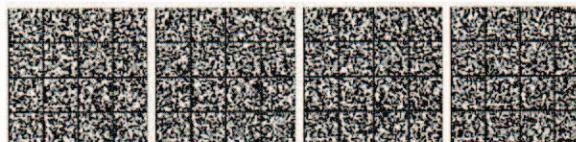
Oltre a XML, per quanto concerne i formati non binari “in chiaro”, è universalmente utilizzato il formato TXT.

Ai fini della conservazione nell’uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.

## 5.8 Formati Messaggi di posta elettronica

Ai fini della conservazione, per preservare l’autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME.

Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui ai precedenti paragrafi.





COMUNE DI SANTA GIUSTINA IN COLLE (PADOVA)

## ELENCO DEI REPERTORI

Repertori del Titolo I "Amministrazione generale":

- Deliberazioni del Consiglio Comunale
- Deliberazioni della Giunta Comunale
- Determinazioni
- Ordinanze
- Decreti Sindacali
- Decreti dei Responsabili
- Atti rogati dal Segretario Comunale (forma pubblica amministrativa)
- Contratti e convenzioni
- Albo Pretorio
- Registro di Protocollo
- Registro delle notifiche
- Albo del volontariato
- Registro denunce infortuni
- Registro deposito atti
- Registro autorizzazioni

Repertori del Titolo IV "Risorse finanziarie":

- Mandati
- Reversali
- Decreti di liquidazione
- Fatture emesse

Repertori del Titolo VI "Pianificazione e gestione del territorio":

- Permessi di costruire, SCIA, DIA

Repertori del Titolo VII "Servizi alla persona":

- Indice dei prestiti

Repertori del Titolo VIII "Attività economiche":

- Registro pratiche SUAP (funzione trasferita alla Federazione dei Comuni del Camposampierese)
- Registro ascensori e montacarichi

Repertori del Titolo X "Tutela della salute":

- Autorizzazioni allo scarico

Repertori del Titolo XI "Servizi demografici":

- Registro dei nati
- Registro dei morti
- Registro dei matrimoni
- Registro di cittadinanza
- Registri immigrazioni/emigrazioni
- Registri AIRE
- Registro carte di identità
- Registro permessi seppellimento
- Registro concessioni cimiteriali
- Registro cremazioni

Repertori del Titolo XII "Elezioni e iniziative popolari":

- Verbali della commissione elettorale comunale
- Verbali dell'ufficiale elettorale comunale

Allegato n. 4

## ELENCO DELLE UNITA' ORGANIZZATIVE DELL'ENTE ED ELENCO UFFICI CON ABILITAZIONI ALLA PROTOCOLLAZIONE

### AREA ORGANIZZATIVA OMOGENEA

DENOMINAZIONE ENTE	COMUNE DI SANTA GIUSTINA IN COLLE (PD)
CODICE IDENTIFICATIVO	c_i207
A.O.O.	COMUNE DI SANTA GIUSTINA IN COLLE
INDIRIZZO DI POSTA ELETTRONICA ISTITUZIONALE	sgcolle@comunesgcolle.pd.it
INDIRIZZO DI POSTA ELETTRONICA CERTIFICATA ISTITUZIONALE	comune.sgcolle.pd@pecveneto.it
TELEFONO	0499304400
FAX	0499304401
WEB	www.comunesgcolle.gov.it

UNITA' ORGANIZZATIVA (U.O.)	SERVIZIO	ABILITAZIONI ALLA PROTOCOLLAZIONE
SETTORE ECONOMICO-FINANZIARIO-AFFARI GENERALI	Segreteria e Protocollo	Registrazioni: Entrata/Uscita/Interno Visibilità: totale
	Ragioneria e Personale	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
	Tributi	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate al servizio
	Servizi Sociali	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
U.O.	SERVIZIO	ABILITAZIONI ALLA PROTOCOLLAZIONE
SETTORE SERVIZI DEMOGRAFICI-CULTURALI- POLITICHE SOCIALI	Anagrafe/stato civile/elettorale	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
	Cultura e Pubblica Istruzione	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
	Politiche Sociali	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
U.O.	SERVIZIO	ABILITAZIONI ALLA PROTOCOLLAZIONE
SETTORE URBANISTICA E AMBIENTE	Edilizia Privata e Ambiente	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate
U.O.	SERVIZIO	ABILITAZIONI ALLA PROTOCOLLAZIONE
SETTORE LAVORI PUBBLICI E MANUTENZIONI	Lavori Pubblici e Manutenzioni	Registrazioni: Uscita/Interno Visibilità: registrazioni assegnate



COMUNE DI SANTA GIUSTINA IN COLLE  
Provincia di Padova

---

Allegato n. 5

**PROTOCOLLO DI EMERGENZA**  
**A NORMA ARTICOLO 63 DEL DPR 445/2000**  
**Breve guida per l'attivazione**

---

Per attivare il registro di protocollo di emergenza si devono verificare tre condizioni, non necessariamente dipendenti una dall'altra:

- 1** guasto al software di protocollazione informatica;
- 2** guasto al sistema informatico di gestione;
- 3** mancanza di energia elettrica.

Quando si verifica la condizione numero 1 si deve attivare un protocollo di emergenza su supporto informatico.

Quando si verificano le condizioni numeri 2 e 3 si deve attivare un protocollo di emergenza su supporto cartaceo.

Per l'attivazione del protocollo di emergenza si deve:

- a)** redigere il verbale di attivazione (documento n. 5.1)
- b)** compilare il registro di emergenza [su supporto informatico manuale (documento n. 5.2);
- c)** dare comunicazione alla struttura organizzativa dell'amministrazione della attivazione dell'emergenza;

Al termine dell'emergenza si deve:

- a)** revocare l'autorizzazione al protocollo di emergenza (documento n. 5.3)
- b)** inserire le registrazioni di emergenza nel protocollo informatico attivando l'apposita funzione, come previsto dal manuale operativo;
- c)** dare comunicazione alla struttura organizzativa dell'amministrazione della revoca dell'emergenza;
- d)** conservare il registro di emergenza.

La numerazione del registro di emergenza è unica per l'intero anno. Ricomincia dal numero successivo all'ultimo generato per ogni attivazione.

Nel caso di attivazione del protocollo manuale (documento n. 5.2) si possono utilizzare registri manuali o fogli singoli con numerazione indicata nel margine destro. La numerazione indicata deve essere riportata per ogni documento registrato.



COMUNE DI SANTA GIUSTINA IN COLLE  
Provincia di Padova

Allegato 5.1

**AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI  
REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA.  
(art. 63 D. P. R. 445/2000)**

Ai sensi dell'art. 63 del D. P. R. 445 del 28 dicembre 2000:

- preso atto che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa dell'interruzione	

Non è possibile utilizzare la normale procedura informatica;

- si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Santa Giustina in Colle, lì

IL RESPONSABILE DEL SERVIZIO





Allegato n. 5.2

***REGISTRO DI EMERGENZA***  
COMUNE DI SANTA GIUSTINA IN COLLE (PADOVA)



COMUNE DI SANTA GIUSTINA IN COLLE  
Provincia di Padova

Allegato 5.3

**REVOCA AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI  
REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA.  
(art. 63 D.P.R. 445/ 2000)**

Ai sensi dell'art. 63 del D. P. R. 445 del 28 dicembre 2000:

- ricordato che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa dell'interruzione	

non essendo possibile utilizzare la normale procedura informatica, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

- preso atto che, dalla data ed ora sotto riportate:

Data ripristino	
Ora ripristino	

è stato ripristinato il normale funzionamento della procedura informatica;

- si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;
- si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Santa Giustina in Colle, lì

IL RESPONSABILE DEL SERVIZIO

## **TITOLARIO ASTENGO (1897)**

### **Categoria I – Amministrazione**

Classe

1. Ufficio Comunale
2. Archivio
3. Economato
4. Elezioni amministrative – Liste – Riparto consiglieri per frazioni
5. Sindaco – Assessori – Consiglieri
6. Impiegati – Inservienti – Personale avventizio, ecc.
7. Locali per gli uffici
8. Sessioni ordinarie e straordinario del consiglio – Deliberazioni
9. Cause – Liti – Conflitti riguardanti l'Amministrazione comunale
10. Andamento dei servizi amministrativi
11. Inchieste
12. Istituti diversi amministrati dal Comune

### **Categoria II – Opere pie e beneficenza**

Classe

1. Congregazione di carità – Opere pie – Monti frumentari – Monti di pietà
2. Ospizi – Ricoveri di mendicanti – Indigenti inabili al lavoro
3. Brefotrofi – Orfanotrofi – Esposti - Baliatici
4. Società operaie e di mutuo soccorso – Sussidi
5. Lotterie – Tombole – Fiere di beneficenza, ecc.

### **Categoria III – Polizia urbana e rurale**

Classe

1. Personale – Guardie municipali – Guardie campestri – Facchini ecc.
2. Servizi – Regolamenti

### **Categoria IV – Sanità ed igiene**

Classe

1. Ufficio sanitario – Personale
2. Servizio sanitario
3. Epidemie – malattie contagiose – epizoozie
4. Sanità marittima - Lazzaretti
5. Igiene pubblica – regolamenti – macello
6. Polizia mortuaria – Cimiteri, ecc.

### **Categoria V – Finanze**

Classe

1. Proprietà comunali – Inventari dei beni mobili e immobili – Debiti e crediti
2. Bilanci – conti – contabilità speciali – verifiche di cassa
3. Imposte, tasse, diritti – Regolamenti, tariffe e ruoli relativi
4. Dazi
5. Catasto

6. Privativa
7. Mutui
8. Eredità
9. Servizio di esattoria e tesoreria

#### **Categoria VI – Governo**

##### Classe

1. Leggi e decreti – Gazzetta ufficiale – Calendario generale dello Stato – Fogli degli Annunzi legali – Circolari
2. Elezioni politiche – Liste
3. Feste nazionali, commemorazioni, ecc
4. Azioni di valore civile
5. Concessioni governative

#### **Categoria VII – Grazia, giustizia e culto**

##### Classe

1. Circoscrizione giudiziaria – Pretura – Tribunale – Corte di Assise
2. Giurati
3. Carceri mandamentali
4. Conciliatore – Vice-conciliatore – ufficio
5. Archivio notarile
6. Culto

#### **Categoria VIII – Leva e truppe**

##### Classe

1. Leva di terra e di mare
2. Servizi militari
3. Tiro a segno
4. Caserme militari

#### **Categoria IX – Istruzione pubblica**

##### Classe

1. Autorità scolastiche – Insegnanti
2. Asili d'infanzia e scuole elementari – Monte pensioni
3. Educatori comunali
4. Ginnasi – Convitti
5. Licei
6. Scuole tecniche
7. Università
8. Istituti scientifici – Biblioteche - Gallerie – Musei, ecc.

#### **Categoria X – Lavori e servizi pubblici – Poste – Telegrafi – Telefoni**

##### Classe

1. Strade – Piazze – Costruzione e manutenzione
2. Ponti
3. Illuminazione
4. Acque e fontane pubbliche
5. Consorzi stradali e idraulici

6. Espropriazioni per cause di utilità pubblica
7. Poste – Telegrafi – Telefoni
8. Ferrovia
9. Ufficio tecnico
10. Restauro e manutenzione edifici
11. Porti – contributi

### **Categoria XI – Agricoltura, industria e commercio**

#### Classe

1. Agricoltura – Caccia – Pesca – Pastorizia – Bachicoltura – Malattie delle piante, ecc.
2. Industria
3. Commercio
4. Fiere e mercati
5. Pesi e misure

### **Categoria XII – Stato civile – Censimento – Statistica**

#### Classe

1. Stato civile
2. Censimento
3. Statistica

### **Categoria XIII – Esteri**

#### Classe

1. Comunicazioni con l'estero
2. Emigrati
3. Emigranti

### **Categoria XIV – Oggetti diversi**

#### Classe Unica

In questa categoria sono classificati tutti gli affari che non trovano posto nelle categorie precedenti e nella quindicesima.

### **Categoria XV – Sicurezza pubblica**

#### Classe

1. Pubblica incolumità
2. Polveri e materie esplodenti
3. Teatri e intrattenimenti pubblici
4. Esercizi pubblici
5. Scioperi e disordini
6. Mendicizia
7. Pregiudicati, ammoniti, sorvegliati, domiciliati coatti, espulsi dall'estero, reduci dalle case di pena, oziosi, vagabondi – Informazioni e provvedimenti
8. Avvenimenti straordinari e affari vari interessanti la P.S.
9. Contributo nella spesa delle guardie di città e casermaggio
10. Trasporto mentecatti al manicomio
11. Incendi e Pompieri

# TITOLARIO

(Piano di classificazione)



*COMUNE DI SANTA GIUSTINA IN COLLE (PADOVA)*

## **Titolo I. Amministrazione generale**

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

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

Classi
1. Sindaco
2. Vice-sindaco
3. Consiglio
4. Presidente del Consiglio
5. Conferenza dei capigruppo e Commissioni del Consiglio
6. Gruppi consiliari
7. Giunta
8. Commissario prefettizio e straordinario
9. Segretario e Vice-segretario
10. Direttore generale e dirigenza
11. Revisori dei conti
12. Difensore civico
13. Commissario <i>ad acta</i>
14. Organi di controllo interni
15. Organi consultivi
16. Consigli circoscrizionali
17. Presidenti dei Consigli circoscrizionali
18. Organi esecutivi circoscrizionali
19. Commissioni dei Consigli circoscrizionali
20. Segretari delle circoscrizioni
21. Commissario <i>ad acta</i> delle circoscrizioni
22. Conferenza dei Presidenti di quartiere



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

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

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

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

### **Titolo V. Affari legali**

Classi
1. Contenzioso

2. Responsabilità civile e patrimoniale verso terzi; assicurazioni
3. pareri e consulenze

## Titolo VI. Pianificazione e gestione del territorio

Classi
1. Urbanistica: piano regolatore generale e varianti
2. Urbanistica: strumenti di attuazione del piano regolatore generale
3. Edilizia privata
4. Edilizia pubblica
5. Opere pubbliche
6. Catasto
7. Viabilità
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
9. Ambiente: autorizzazioni, monitoraggio e controllo
10. Protezione civile ed emergenze

## Titolo VII. Servizi alla persona

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

## Titolo VIII. Attività economiche

Classi
1. Agricoltura e pesca
2. Artigianato
3. Industria
4. Commercio
5. Fiere e mercati

6. Esercizi turistici e strutture ricettive
7. Promozione e servizi

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

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

**Titolo X. Tutela della salute**

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

**Titolo XI. Servizi demografici**

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

**Titolo XII. Elezioni e iniziative popolari**

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

**Titolo XIII. Affari militari**

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

<b>Titolo XIV. Oggetti diversi</b>
------------------------------------

## OGGETTO: RICHIESTA DI ACCESSO ALL'ARCHIVIO STORICO

Al Sig. Sindaco  
del Comune di  
SANTA GIUSTINA IN COLLE

In applicazione degli artt. 38, 102, 103 e 122 del Codice dei Beni Culturali e del Paesaggio (D. Lgs. 42 del 22.01.2004)

Il/La sottoscritt... Cognome e nome \_\_\_\_\_

Nato a \_\_\_\_\_ il \_\_\_\_\_

Residente a \_\_\_\_\_ in Via/Piazza \_\_\_\_\_

Telefono \_\_\_\_\_ e-mail \_\_\_\_\_

Chiede di consultare i seguenti documenti dell'Archivio

.....  
.....

Per la seguente motivazione di studio o ricerca:

.....

Relativi al periodo storico.....

Data ..... (firma leggibile) \_\_\_\_\_

VISTO SI AUTORIZZAZIONE:  
IL RESPONSABILE DEL SERVIZIO

Data e firma \_\_\_\_\_



## **Manuale dei processi di formazione e conservazione dei documenti elettronici**

**COMUNE DI SANTA GIUSTINA IN COLLE (PD)**



Data versione 28/09/2015

Versione 02

Redatto da Comune di Santa  
Giustina in Colle

Approvato da GIUNTA  
COMUNALE N. 102 del  
28/09/2015

**INDICE**

<b>1</b>	<b>Introduzione al documento.....</b>	<b>5</b>
1.1	Gestione versioni documento .....	5
1.2	Scopo e campo di applicazione del documento.....	5
1.3	Principi di redazione.....	6
1.4	Termini e definizioni .....	6
1.5	Acronimi.....	8
<b>2</b>	<b>Nomine e individuazione dei compiti.....</b>	<b>9</b>
2.1	Cliente.....	9
2.2	Referenti di processo.....	9
2.3	Responsabile della conservazione .....	10
2.4	InfoCert SPA.....	10
2.4.1	Identificazione del sistema di conservazione .....	11
2.4.2	Supporto offerto dal sistema di conservazione.....	11
<b>3</b>	<b>Fondamenti normativi .....</b>	<b>12</b>
3.1	Introduzione .....	12
3.2	Il quadro normativo .....	12
3.3	Principali riferimenti normativi .....	12
3.4	La conservazione sostitutiva dei documenti .....	13
3.5	La deliberazione CNIPA n. 11 del 19 febbraio 2004.....	15
3.6	Il responsabile della conservazione .....	15
3.7	La normativa in pratica.....	16
<b>4</b>	<b>Il sistema di creazione e gestione dei documenti.....</b>	<b>17</b>
4.1	Strumenti utilizzati.....	17
4.1.1	Servizi di certificazione .....	17
4.2	Controlli.....	17
4.3	Indicizzazione dei documenti .....	18
4.4	Gestione delle anomalie .....	18
4.5	Formato dei documenti elettronici.....	18
<b>5</b>	<b>Il sistema di conservazione documentale .....</b>	<b>19</b>
5.1	Descrizione generale del servizio .....	19
5.2	Definizione di documento.....	19
5.3	Configurazione dei sistemi.....	20

5.3.1	Modalità di erogazione .....	20
5.4	Componenti.....	20
5.4.1	Marca temporale.....	20
5.4.2	Firma digitale con dispositivo HSM .....	21
5.4.3	Supporti di conservazione .....	21
5.4.4	Posta Elettronica Certificata .....	21
5.5	Controlli.....	21
5.5.1	Controlli di processo .....	21
5.5.2	Controlli periodici.....	22
5.5.3	Ispezione del sistema da parte delle autorità competenti.....	22
5.5.4	Incident management.....	22
<b>6</b>	<b>Le tipologie documentali .....</b>	<b>23</b>
6.1	Contratti .....	23
6.2	Atti Amministrativi .....	23
6.3	Allegati .....	23
6.3.1	Fasi del processo .....	24
<b>7</b>	<b>Il processo di conservazione.....</b>	<b>26</b>
7.1	Processi di front-end.....	26
7.2	Processi di back-end.....	26
7.3	Fasi del processo di conservazione: schema generale .....	27
7.4	Responsabilità del processo di conservazione .....	27
7.5	Fasi del processo di conservazione: dettaglio .....	28
7.5.1	Formazione del documento .....	28
7.5.2	Indicizzazione e archiviazione .....	28
7.5.3	Acquisizione documento e creazione del file delle direttive .....	29
7.5.4	Invio al sistema di conservazione.....	29
7.5.5	Verifica, accettazione e invio della ricevuta di accettazione del documento .....	29
7.5.6	Inserimento nel lotto e creazione del file di controllo.....	30
7.5.7	Chiusura del lotto e attestazione di corretto procedimento .....	30
7.5.8	Memorizzazione, creazione copia di sicurezza e chiusura della conservazione.....	30
<b>8</b>	<b>Procedure di ricerca ed esibizione.....</b>	<b>32</b>
8.1	Procedura di esibizione: schema generale.....	32
8.2	Procedura di esibizione: dettaglio .....	33
8.2.1	Ricerca del documento da esibire .....	33
8.2.2	Invio della richiesta a LegalDoc.....	33
8.2.3	Ricerca del documento nel sistema ed esibizione.....	33
8.2.4	Verifica del documento .....	33
8.2.5	Verifica del documento .....	34
8.3	Requisiti software.....	34
<b>9</b>	<b>Modifica dei documenti posti in conservazione .....</b>	<b>35</b>





9.1	La cancellazione di un documento.....	35
<b>10</b>	<b>Misure di sicurezza.....</b>	<b>36</b>
10.1	Comune di S.Giustina in Colle.....	36
10.2	InfoCert.....	36
10.2.1	Sicurezza fisica.....	36
10.2.2	Gruppi di continuità.....	36
10.2.3	Connessione a Internet .....	36
10.2.4	Sicurezza delle reti: protezione da intrusioni.....	37
<b>11</b>	<b>Note conclusive .....</b>	<b>38</b>
11.1	Procedure di riversamento .....	38
11.1.1	Riversamento diretto .....	38
11.1.2	Riversamento sostitutivo .....	38
11.2	Protezione dei dati personali .....	38
<b>12</b>	<b>Allegati.....</b>	<b>39</b>
12.1	Documentazione contrattuale di riferimento.....	39

## 1 Introduzione al documento

### 1.1 Gestione versioni documento

Versione:	02	Data Versione:	28/09/2015
Descrizione modifiche:	attivazione nuova classe documentale "Registro di protocollo" e aggiornamento lista firme digitali utilizzate		
Motivazioni:	Revisione		

### 1.2 Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti (di seguito anche "Manuale della Conservazione") ai sensi dell'articolo 62 del Manuale di Gestione dei documenti ex art. 5 DPCM 31 ottobre 2000 redatto dal Comune di Santa Giustina in Colle (PD)

Il Manuale ha lo scopo di raccogliere le diverse normative in materia e di documentare il processo di conservazione dei documenti elettronici.

Inoltre, descrive tutte le procedure e le prassi seguite dal Comune di Santa Giustina in Colle (PD) (di seguito anche "Comune") in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate: questa parte costituisce il regolamento operativo di tutti i processi di digitalizzazione dei documenti di conservazione digitale.

In caso di ispezione da parte delle Autorità di Vigilanza o di altri organismi a ciò deputati, il Manuale permette un agevole svolgimento di tutte le attività di controllo e costituisce una importante dimostrazione dell'impegno dell'Ente al rispetto delle norme.

Il documento si applica al servizio LegalDoc fornito in modalità ASP (Application Service Providing) da InfoCert SpA secondo uno schema di Business Process Outsourcing (BPO).

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-3) contiene una panoramica di tutte le leggi e i decreti che regolano la materia, fornisce il profilo del Comune di Santa Giustina in Colle (PD), il profilo di InfoCert e dettaglia la configurazione dei sistemi utilizzati per l'erogazione;
2. la seconda sezione (capitoli 4-9) descrive il servizio LegalDoc, il responsabile della conservazione, descrive i macro flussi operativi definiti per la gestione della documentazione elettronica. Inoltre, è dettagliato il procedimento di conservazione posto sotto la responsabilità di InfoCert in virtù della delega allo svolgimento delle attività di competenza del Responsabile della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi ricerca e esibizione a norma dei documenti conservati.
3. la terza sezione (capitoli 10-12) riporta le misure fisiche e logiche di sicurezza adottate, cenni sui riversamenti, i riferimenti alla normativa e alla policy sulla protezione dei dati personali e gli allegati al Manuale.

### 1.3 Principi di redazione

La redazione del Manuale della Conservazione del Comune di Santa Giustina in Colle (PD) è ispirata ai seguenti principi:

- **Principio di Trasparenza**, il Manuale mira a fornire una chiara spiegazione del sistema di conservazione documentale e dei processi erogati;
- **Ottica di processo**, il documento mira a descrivere le fasi del processo, non il dettaglio tecnico degli strumenti utilizzati, ad uso interno e a fini ispettivi;
- **Principio di Rilevanza**: nel Manuale sono contenute solamente le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, senza dettagli tecnici superflui;
- **Principio di Accuratezza**: le informazioni sono state revisionate da più persone, poste ai diversi livelli della catena decisionale.

### 1.4 Termini e definizioni

<b>ARCHIVIAZIONE</b>	è il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
<b>CONSERVAZIONE SOSTITUTIVA</b>	vedi conservazione
<b>CONSERVAZIONE</b>	il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nella deliberazione CNIPA 11 del 19 febbraio 2004.
<b>DOCUMENTO ANALOGICO ORIGINALE</b>	documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
<b>DOCUMENTO INFORMATICO</b>	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
<b>DATI SENSIBILI</b>	ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196 e la seguente deliberazione del Consiglio dei Ministri del 25 maggio 2012, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
<b>EVIDENZA INFORMATICA</b>	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1 comma 1 lettera r) deliberazione CNIPA 11 del 19 febbraio 2004)

<b>FIRMA DIGITALE</b>	un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82)
<b>FIRMA ELETTRONICA</b>	l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82)
<b>FIRMA ELETTRONICA QUALIFICATA</b>	un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82)
<b>FIRMA ELETTRONICA AVANZATA</b>	insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
<b>IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)</b>	la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art. 1 comma 1 lettera s) deliberazione CNIPA 11 del 19 febbraio 2004).
<b>LOTTO DI DOCUMENTI</b>	insieme di documenti raggruppati secondo un criterio di aggregazione, aventi un file indice (file di chiusura del lotto) che attesta la conservazione con l'apposizione della firma del Responsabile della Conservazione e della marca temporale.
<b>MARCA TEMPORALE</b>	il riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi, definita anche nel DPCM 22 febbraio 2013, titolo IV
<b>PORTABLE DOCUMENT FORMAT</b>	formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.
<b>RESPONSABILE DELLA CONSERVAZIONE</b>	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva conformemente a quanto previsto all'art. 5 della deliberazione Cnipa 11 del 19 febbraio 2004.



<b>RIFERIMENTO TEMPORALE</b>	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009, definito anche nel DPCM 22 febbraio 2013.
<b>HARDWARE SECURITY MODULE</b>	dispositivo crittografico ad alte prestazioni utilizzato per apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici
<b>POSTA ELETTRONICA CERTIFICATA</b>	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
<b>EXTENSIBLE MARKUP LANGUAGE</b>	linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.

## 1.5 Acronimi

<b>CA</b>	Certification Authority
<b>CNIPA</b>	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, successivamente DigitPA ora Agenzia per l'Italia Digitale
<b>D. LGS</b>	Decreto Legislativo
<b>DPCM</b>	Decreto del Presidente del Consiglio dei Ministri
<b>GU</b>	Gazzetta Ufficiale della Repubblica Italiana
<b>HSM</b>	Hardware Security Module
<b>PDF</b>	Portable Document Format
<b>PEC</b>	Posta Elettronica Certificata
<b>SG</b>	Sistema di Gestione
<b>SGD</b>	Sistema di Gestione Documentale
<b>SSL</b>	Secure Socket Layer
<b>TSA</b>	Time Stamping Authority
<b>TSS</b>	Time Stamping Service
<b>TU</b>	Testo Unico
<b>URL</b>	Uniform Resource Locator
<b>XML</b>	Extensible Markup Language

## 2 Nomine e individuazione dei compiti

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei e conservazione elettronica documentale.

### 2.1 Cliente

<b>Ente</b>	Comune di Santa Giustina in Colle (PD)
<b>Sede Amministrativa</b>	Piazza dei Martiri 3 – 35010 Santa Giustina in Colle
<b>Recapiti</b>	0499304400
<b>Sito web</b>	www.comunesgcolle.gov.it
<b>Partita IVA</b>	00949560288
<b>Codice Fiscale</b>	80010030288

### 2.2 Referenti di processo

Nominativo dei soggetti del Comune di Santa Giustina in Colle (PD) incaricati della gestione del sistema di creazione dei documenti e di invio dei documenti in conservazione.

<b>Nome e Cognome</b>	Fiorenza Verzotto - Responsabile della Conservazione interno (Responsabile del Settore Economico-Finanziario-Affari Generali e Responsabile gestione documentale)
<b>Ente/Società</b>	Comune di Santa Giustina in Colle (PD)
<b>Data inizio incarico</b>	Dalla data di adozione del presente Manuale
<b>Data termine incarico</b>	

<b>Nome e Cognome</b>	Flavia Gottardello - Referente di processo (Ufficio Contratti/Segreteria)
<b>Ente/Società</b>	Comune di Santa Giustina in Colle (PD)
<b>Tipologia documentale di competenza</b>	Atti a repertorio
<b>Data inizio incarico</b>	Dalla data di adozione del presente Manuale
<b>Data termine incarico</b>	

<b>Nome e Cognome</b>	Patrizia Smania - Referente di processo (referente interno CED/vicario del Responsabile gestione documentale)
<b>Ente/Società</b>	Comune di Santa Giustina in Colle (PD)
<b>Tipologia documentale di competenza</b>	Atti a repertorio
<b>Data inizio incarico</b>	Dalla data di adozione del presente Manuale

<b>Data termine incarico</b>	
------------------------------	--

### 2.3 Responsabile della conservazione

Il Comune di Santa Giustina in Colle (PD), avvalendosi della facoltà prevista dalla Deliberazione CNIPA 11/2004, articolo 5, commi 2 e 3, ha affidato lo svolgimento delle attività del Responsabile della Conservazione ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle suddette attività (si veda in proposito l'allegato n° [2] Affidamento del procedimento di conservazione sostitutiva).

Le attività sono state affidate ad InfoCert SpA, gestore del servizio di conservazione sostitutiva in outsourcing LegalDoc.

InfoCert assume l'incarico di svolgere le attività delegate dal Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali e dall'articolo 5 della Deliberazione CNIPA 11/2004, che ne delinea i compiti.

InfoCert SpA provvede ad affidare lo svolgimento delle attività delegate dal Responsabile della Conservazione ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali.

L'incaricato di InfoCert può delegare lo svolgimento di parte del processo a una o più persone con adeguata competenza ed esperienza, secondo quanto previsto nella documentazione interna di organizzazione e gestione del servizio di conservazione.

L'atto di affidamento allo svolgimento delle attività del Responsabile della Conservazione viene conferito dal Comune di Santa Giustina in Colle (PD) ad InfoCert contestualmente alla sottoscrizione del contratto di adesione al servizio LegalDoc.

### 2.4 InfoCert SPA

<b>Denominazione sociale</b>	<b>InfoCert SpA</b>
<b>Sede Legale:</b>	Piazza Sallustio, 9 00187 Roma Tel. +39 06 442851 Fax +39 06 44285255
<b>Sedi Operative:</b>	Via Russoli, 5 20143 Milano Tel. +39 02 87286700
	Corso Stati Uniti, 14 35127 Padova Tel. +39 049 8288111 Fax +39 049 8288406
<b>Sito web:</b>	www.infocert.it
<b>e-mail</b>	info@infocert.it
<b>PEC</b>	infocert@legalmail.it
<b>Codice Fiscale / Partita IVA</b>	07945211006
<b>Numero REA</b>	RM - 1064345

InfoCert S.p.A. è il Primo Ente Certificatore per la firma digitale in Italia, leader di mercato per i processi di conservazione sostitutiva dei documenti a norma di legge e per i servizi di Posta Elettronica Certificata.

InfoCert S.p.A. progetta e sviluppa soluzioni informatiche ad alto valore tecnologico per la dematerializzazione dei processi documentali di imprese, associazioni, ordini professionali, Pubblica Amministrazione e professionisti.

InfoCert S.p.A., con un capitale sociale di 17.704.890,00 euro ed un fatturato 2011 di 30 milioni di euro, eroga servizi di gestione documentale (LegalCycle), conservazione sostitutiva a norma dei documenti (LegalDoc), certificazione e sicurezza digitale (LegalCert), gestione di Posta Elettronica Certificata (Legalmail), formazione e conservazione a norma del Libro Unico del Lavoro in formato elettronico (LegalHR), dematerializzazione dei flussi documentali verso le banche (LegalPay) e gestione efficiente e sicura della modulistica elettronica (LegalForm).

Nel dicembre 2009 l'offerta di InfoCert si arricchisce grazie alla acquisizione al 100% di KLever, società di consulenza tecnologica focalizzata su soluzioni di Enterprise Content Management (ECM).

#### **2.4.1 Identificazione del sistema di conservazione**

Il Responsabile della Conservazione InfoCert viene identificato nel sistema LegalDoc grazie alla definizione di un particolare utente con il ruolo di "responsabile del procedimento di conservazione".

Gli estremi identificativi di questo particolare utente (organizzazione di appartenenza, cognome, nome, codice fiscale) sono, inoltre, riportati anche nelle informazioni associate ai documenti conservati (nelle informazioni relative ad ogni documento e nel file di chiusura lotto).

#### **2.4.2 Supporto offerto dal sistema di conservazione**

LegalDoc supporta il Responsabile della Conservazione InfoCert nel controllo dell'effettiva leggibilità dei documenti conservati e mantiene la tracciatura delle esibizioni effettuate, considerate una ulteriore prova di leggibilità.

Il sistema gestisce in maniera automatica i parametri di organizzazione del contenuto dei supporti di memorizzazione e le procedure di sicurezza e di tracciabilità, fondamentali per la corretta conservazione del documento conservato.

Il sistema supporta il Responsabile della Conservazione nell'archiviazione delle informazioni relative a ogni supporto di memorizzazione utilizzato attraverso specifiche funzionalità, sulle quali egli esercita l'attività di controllo e di supervisione.

LegalDoc, inoltre, fornisce al Responsabile della Conservazione InfoCert un set di funzionalità per il mantenimento dell'archivio delle diverse versioni del software in gestione e il monitoraggio sia del flusso di documenti elaborati dal sistema, sia dei server specializzati. Il sistema, infatti, segnala ogni anomalia riscontrata, consentendo un pronto intervento e assicurando un monitoraggio costante.



### 3 Fondamenti normativi

#### 3.1 Introduzione

Le realtà aziendali e di Pubblica Amministrazione avvertono in maniera sempre crescente la necessità di ottenere e gestire informazioni corrette, tempestive, aggiornate, autentiche, integre, logicamente accessibili, protette e disponibili nel tempo. Riuscire a garantire queste caratteristiche permette alla dirigenza di rispondere in maniera adeguata alle richieste interne o esterne all'ente e di trasformarle in un reale vantaggio.

Al crescere dei volumi della documentazione prodotta, il costo per archiviare e conservare nel tempo le informazioni in modo organizzato è ingente e può creare inutili processi di burocratizzazione. Per questi motivi una ben organizzata adozione del documento digitale consente di ridurre i costi e supportare efficacemente l'attività dell'ente.

#### 3.2 Il quadro normativo

Il contesto normativo in cui si inquadra la conservazione sostitutiva risale al 1994, ma è solo a partire dall'anno 2004 che interventi più significativi hanno reso possibile la conservazione dei documenti in formato digitale valevole anche ai fini fiscali. Senza ripercorrere in dettaglio tutto l'excurus legislativo, se ne fornisce di seguito una panoramica per una più agevole comprensione dell'intero quadro normativo.

La legge numero 537 del 24 dicembre 1993 "Interventi correttivi di finanza pubblica" (GU n. 303 del 28 dicembre 1993) affronta per la prima volta il tema di una modalità alternativa di conservare (e conseguentemente esibire) dei documenti a fini amministrativi. La norma introduce nell'ordinamento la possibilità di conservare scritture e documenti contabili "sotto forma di registrazioni su supporti di immagini" ed estende questa possibilità anche a tutte le scritture e i documenti rilevanti ai fini delle disposizioni tributarie.

Le relative modalità operative, tuttavia, sono rimandate ad un decreto del Ministero delle Finanze, emanato solamente dieci anni più tardi (23 gennaio del 2004) permettendo l'avvio concreto del processo.

Nel frattempo, è stato completato il quadro normativo relativo al documento informatico, alla firma digitale e alla fattura elettronica (a titolo non esaustivo si citano il Testo Unico sulla documentazione amministrativa – TU 445/2000, il Decreto del Presidente del Consiglio dei Ministri 8/02/1999 ora sostituito dal Decreto del Presidente del Consiglio dei Ministri del 13/01/2004, le numerose deliberazioni AIPA – poi divenuta CNIPA, ora DigitPA –, il Decreto Ministero Economia e Finanze 23 gennaio 2004 e il Decreto Legislativo 52 del 20 febbraio 2004, relativi a specifiche tipologie di documenti).

Inoltre, è stato emanato il "Codice Dell'Amministrazione digitale", il D.Lgs n. 82 del 7 marzo del 2005 (GU 16/05/2005 s.o. n. 93/L) entrato in vigore a partire dal 1 gennaio 2006, che vuole contribuire a rendere ancora più omogeneo il quadro di riferimento; da questa data tutte le disposizioni non riunite e coordinate all'interno del Codice sono state abrogate. Il Codice è stato recentemente rivisto dal D.Lgs. n. 235 del 30 dicembre 2010, allo scopo di rendere il quadro normativo più coerente alle innovazioni tecnologiche occorse negli ultimi anni.

#### 3.3 Principali riferimenti normativi

1. *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445* – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Testo coordinato con le modifiche apportate dal D.Lgs 23 gennaio 2002, n. 10 e dal DPR 7 aprile 2003, n. SQ01-00-02 Procedura per la gestione della documentazione.

Questo DPR è stato per la maggior parte sostituito dal Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006.



2. *Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche* – Codice in materia di Protezione dei Dati Personali
3. *Decreto del 23 gennaio 2004 del Ministero dell'Economia e delle Finanze* – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.
4. *Deliberazione CNIPA n. 11 del 19 febbraio 2004* – Regole tecniche per la riproduzione e conservazione su supporto ottico idoneo a garantire al conformità dei documenti agli originali.
5. *Decreto Legislativo del 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale* – Testo che rappresenta la base per tutti i successivi interventi che verranno in tema di uso dei documenti digitali. In dettaglio si definiscono nuovamente i ruoli e le caratteristiche dei documenti informatici e se ne amplia l'utilizzo; in particolare, la PA vede imporre un uso delle tecnologie informatiche e la pressoché totale dematerializzazione dei documenti nei rapporti tra cittadini, imprese e pubblica amministrazione.
6. *Decreto-Legge 29 novembre 2008, n. 185, coordinato con la legge di conversione 28 gennaio 2009, n. 2 – Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale* – Modifiche al CAD in materia di copie informatiche di documenti analogici, modifiche al Codice Civile in materia di documentazione informatica
7. *Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009* – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
8. *Decreto Legislativo del 30 dicembre 2010* – Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
9. *Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013* - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 (GU n.117 del 21-5-2013).
10. Il Decreto denominato sviluppo-bis, (dl 179/2012 convertito in legge 221/2012) modificando l'articolo 11, comma 13, del Codice dei contratti pubblici (D.L.vo 163/2006), ha introdotto nell'ordinamento l'obbligo che i contratti della pubblica amministrazione si stipulino esclusivamente in forma elettronica e non cartacea, almeno quando siano stipulati per atto pubblico notarile o in forma pubblica amministrativa. La nuova regolamentazione delle forme specifiche della stipulazione ha efficacia a partire dal 1° gennaio 2013 (data di efficacia dell'innovazione normativa, come esplicitato dallo stesso articolo 6, comma 4 della legge 221/2012).
11. *Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014* – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20,22,23-bis, 23-ter,40 comma 1 e 71, comma 1, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (G.U. n. 8 del 12/01/2015).
12. *Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013* – Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005 (supplemento n. 20 alla G.U. n. 59 del 12/03/2014).

### 3.4 La conservazione sostitutiva dei documenti

L'implementazione e la gestione dei processi di creazione e conservazione dei documenti elettronici e di conservazione sostitutiva è una operazione che si avvale di numerosi strumenti ed elementi, regolata da apposite discipline che vanno ricollegate alla disciplina generale della conservazione.

Di seguito si richiamano i principali strumenti ed elementi:

- **Documento informatico:** è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso.

Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano garantite, in particolare, l'integrità e l'autenticità. Esemplicando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
- **Documento analogico:** in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfiche e microfilm, nastro audio e video. Il documento analogico può essere originale, a sua volta distinto in originale unico e non unico, o copia.
- **Supporto di memorizzazione:** il supporto può essere ottico o non ottico, in quanto il documento esiste a prescindere dal supporto su cui è memorizzato. La deliberazione CNIPA 11/2004 autorizza l'utilizzo di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser (dischi ottici WORM e CD-R, dischi magneto-ottici o DVD). È data, inoltre, la possibilità di utilizzare un qualsiasi altro supporto di memorizzazione, oltre a quelli a tecnologia laser, nel rispetto delle regole tecniche previste ed in mancanza di altri motivi ostativi.

Si è, infatti, raggiunta la consapevolezza del fatto che gli strumenti di firma digitale e di marca temporale garantiscono idoneamente l'integrità del documento nel processo di conservazione, indipendentemente dal supporto scelto. Gli stessi strumenti garantiscono anche la possibilità di trasmissione telematica dei documenti, senza che questo processo di trasmissione possa portare ad alterazioni di sorta.
- **Firma digitale:** è l'elemento principale che interviene nella gestione elettronica del documento informatico dalla formazione, alla trasmissione, fino alla conservazione, poiché conferisce piena validità legale al documento cui è apposta, assicurando autenticità, integrità, non ripudiabilità.
- **Attestazione temporale:** per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere questo risultato è la marca temporale, una particolare firma elettronica che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

Il fine ultimo del processo di conservazione è rendere un documento inalterabile ed imm modificabile, in modo che possa essere disponibile nel tempo nella propria autenticità ed integrità.

In linea generale non sono previste autorizzazioni preventive per l'adozione di criteri operativi per effettuare la conservazione sostitutiva. Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali, tuttavia, è necessario rispettare le regole tecniche previste dalla normativa, previste nella deliberazione CNIPA n. 11 del 19 febbraio 2004, in vigore dal 9 marzo 2004 ed integrate, per quanto concerne i documenti rilevanti ai fini tributari, dal Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze.

### 3.5 La deliberazione CNIPA n. 11 del 19 febbraio 2004

La deliberazione CNIPA 11/2004 detta le regole valide, in generale, per le procedure per la riproduzione e conservazione dei documenti su supporto idoneo a garantire la conformità dei documenti agli originali.

La deliberazione, che sostituisce integralmente la precedente numero 42 del 2001, aggiorna le regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, come previsto all'articolo 6, commi 1 e 2, del TU delle disposizioni legislative e regolamentari in materia di documentazione amministrativa di cui al DPR 28 dicembre 2000, n. 445.

Il provvedimento ridefinisce il quadro normativo di riferimento, mutato grazie al progresso tecnologico, adattandolo alle nuove situazioni.

### 3.6 Il responsabile della conservazione

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) enfatizza il ruolo del Responsabile della Conservazione di documenti in formato digitale che assume un ruolo fondamentale all'interno del processo di conservazione sostitutiva, insieme ai suoi delegati o ai terzi affidatari.

La presenza del Responsabile della Conservazione è necessaria sia in ambito privato sia in ambito pubblico e vi sono attribuiti compiti debitamente elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Il Responsabile della Conservazione è tenuto a gestire il processo in coerenza con quanto stabilito dalla normativa in vigore.

Uno dei obiettivi principali del Responsabile della Conservazione sostitutiva è di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione sostitutiva.

Più in particolare dovrà provvedere a:

1. definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, tenendone evidenza;
2. organizzare conseguentemente il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche al fine consentire l'esibizione di ciascun documento conservato;
3. archiviare e rendere disponibili, con l'impiego di procedure elaborative e relativamente ad ogni supporto di memorizzazione utilizzato:
  - a) la descrizione del contenuto dell'insieme dei documenti;
  - b) gli estremi identificativi del Responsabile della Conservazione;
  - c) gli estremi identificativi delle persone eventualmente delegate dal Responsabile della Conservazione, con l'indicazione dei compiti alle stesse assegnati;
  - d) l'indicazione delle copie di sicurezza.
4. mantenere e rendere accessibile un archivio dei programmi in gestione nelle eventuali diverse versioni;
5. verificare la corretta funzionalità del sistema e dei programmi in gestione;
6. adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
7. richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività attribuitegli;
8. definire e documentare le procedure da rispettare per l'apposizione del riferimento temporale;
9. verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Al Responsabile della Conservazione sono attribuiti compiti cruciali in ragione del controllo e della supervisione che egli attua sull'intero procedimento di conservazione sostitutiva.

Gli adempimenti comprendono non solo attività di pianificazione, ma anche attività di tipo operativo/esecutivo, che può essere necessario svolgere in sedi diverse e magari distanti tra di loro. L'utilizzo degli strumenti telematici, infatti, consente di memorizzare documenti e scritture contabili con estrema facilità e a costi minori in sedi accentrate specializzate.

La deliberazione CNIPA 11/2004 ai commi 2 e 3 dell'art. 5 consente di delegare in tutto o in parte le attività previste ad altri soggetti interni alla struttura e/o di affidarle a soggetti terzi (pubblici o privati) i quali sono tenuti ad osservare le disposizioni contenute nella deliberazione stessa.

### 3.7 La normativa in pratica

<i>Tipologia</i>	<i>Emissione</i>	<i>Conservabile in modalità sostitutiva</i>
Documento cartaceo "non unico"	Cartacea	Sì
Documento cartaceo "unico"	Cartacea	Sì, con l'intervento del Pubblico Ufficiale
Documento elettronico semplice	Nessuna condizione (la sua validità è sottoposta alla valutazione del giudice)	Sì
Documento elettronico con valenza di "forma scritta"	Documento "statico" Firma elettronica qualificata o firma digitale	Sì

## 4 Il sistema di creazione e gestione dei documenti

I documenti vengono creati mediante sistemi di videoscrittura in uso presso l'Ente in maniera statica e non modificabile; vengono poi firmati digitalmente da controparti e responsabili.

Si rimanda al Manuale di Gestione che il Comune di Santa Giustina in Colle (PD) dovrà approvare per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti, con particolare riferimento alle modalità di utilizzo dello stesso.

### 4.1 Strumenti

#### 4.1 Strumenti utilizzati

Per la redazione dei documenti gli operatori utilizzano i software di videoscrittura Microsoft Word e Open Office. La trasformazione in pdf o pdf-A è effettuata con l'applicativo Pdf Creator anche direttamente dai gestionali.

##### 4.1.1 Servizi di certificazione

Il Segretario Comunale, i Responsabili dei Servizi ed i dipendenti sottoelencati sono dotati di firma digitale (utilizzano le businessKeys):

PONTINI CLAUDIO – Segretario Comunale – BusinessKey Infocert scadenza 11.04.2017

GALLO PAOLO – Sindaco - BusinessKey Infocert scadenza 9.06.2017

VERZOTTO FIORENZA – Responsabile Settore Economico-Finanziario-Affari Generali - BusinessKey Infocert scadenza 13.12.2015

FRANCO SILVANA – Responsabile Settore Urbanistica - BusinessKey Infocert scadenza 13.12.2015

PASQUIN GUIDO – Responsabile Settore LL.PP - BusinessKey Infocert scadenza 13.12.2015

SMANIA PATRIZIA – Istruttore Direttivo Ufficio Ragioneria/CED – BusinessKey Infocert scadenza 10.03.2017

RIZZO PAOLA – Istruttore Ufficio Ragioneria - BusinessKey Infocert scadenza 10.03.2017

CHIARION MARIA ANTONELLA – Collaboratore Servizi Demografici – BusinessKey Infocert scadenza 10.03.2017

MOROSINOTTO MANOLA – Istruttore Servizi Demografici - BusinessKey Infocert scadenza 10.03.2017

PALLARO SILVIA – Esecutore Ufficio Protocollo - BusinessKey Infocert scadenza 10.03.2017

ZARPELLON ANGELA - Messo – BusinessKey Infocert scadenza 10.03.2017

SILVIA RUFFATO – Presidente del Consiglio Comunale – Token USB-ARUBA SPA scadenza 15/04/2020

#### 4.2 Controlli

Ai sensi di legge, il Comune di Santa Giustina in Colle (PD) assicura che i documenti inviati in conservazione sono statici non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.



#### 4.3 Indicizzazione dei documenti

Il Comune di Santa Giustina in Colle (PD) provvede all'indicizzazione dei documenti utilizzando le funzioni messe a disposizione dal sistema di creazione e gestione dei documenti.

#### 4.4 Gestione delle anomalie

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e dimensioni non superiori ai 50 MB. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità per LegalDoc di accettare il documento, lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia al Comune di Santa Giustina in Colle (PD).

#### 4.5 Formato dei documenti elettronici

La Deliberazione CNIPA numero 11/2004 non elenca in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti, ovvero le modalità di organizzazione delle informazioni in un codice binario.

Per questa ragione il Comune di Santa Giustina in Colle (PD) ha preferito individuare i formati specifici nei quali creare i propri documenti elettronici facendo riferimento all'Allegato 2 - Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici Versione del 05/08/2011 – BOZZA (Rif. Sito <http://www.digitpa.gov.it/codice-amministr-digitale/attuazione-del-cad> "Il 5 agosto 2011 è stata pubblicata la bozza delle regole tecniche in materia di documento informatico, gestione documentale e sistema di conservazione dei documenti informatici per l'avvio della fase di consultazione pubblica che si è conclusa in data 10 settembre 2011. L'esame dei commenti e contributi ricevuti, di cui si ringraziano i partecipanti, hanno portato alla stesura di una versione aggiornata della bozza di regole tecniche che sarà definitiva solo a seguito della conclusione dell'iter legislativo con la pubblicazione su Gazzetta Ufficiale".) Il DPCM 13 novembre 2014 "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici della pubbliche amministrazioni ai sensi degli articoli 20,22,23-bis, 23-ter,40 comma 1 e 71, comma 1, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005" è stato pubblicato nella G.U. n. 8 del 12/01/2015.

## 5 Il sistema di conservazione documentale

### 5.1 Descrizione generale del servizio

LegalDoc è un servizio di conservazione dei documenti erogato in modalità ASP e sviluppato sulle esigenze di imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale, che permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

LegalDoc consente le funzionalità di:

- conservazione del documento: il documento, ricevuto negli Internet Data Center di InfoCert in formato digitale statico non modificabile, ovvero redatto in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso, viene conservato a norma di legge per tutta la durata prevista dal contratto;
- rettifica di un documento conservato: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica non comporta la cancellazione del documento originario dall'archivio a norma ma è una modifica logica, nel pieno rispetto del principio di tracciabilità del documento;
- cancellazione di un documento conservato: un documento inviato in conservazione può essere cancellato, allegando eventualmente la motivazione della cancellazione. Il sistema terrà comunque traccia del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità del documento;
- visualizzazione di un documento conservato (esibizione a norma): il documento richiesto viene richiamato via web direttamente dal servizio di conservazione sostitutiva LegalDoc ed esibito con garanzia della sua opponibilità a terzi.

LegalDoc integra il sistema di gestione documentale in uso dal Comune di Santa Giustina in Colle (PD) e ne estende i servizi con funzionalità di stoccaggio digitale; il servizio consente di organizzare liberamente le fasi di creazione, utilizzo e archiviazione dei documenti, intervenendo solamente nella fase di conservazione e solamente per i documenti che l'azienda sceglie di conservare.

### 5.2 Definizione di documento

In LegalDoc il documento è un insieme di uno o più file digitali, anche di diverse tipologie. Ad ogni documento è associato un file di controllo e un file delle direttive di conservazione, nonché un identificativo univoco generato da LegalDoc ("Token LegalDoc"). Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre da LegalDoc parti di un documento.

Un documento conservato presso il sistema LegalDoc, quindi, ha le seguenti caratteristiche:

- è costituito da uno o più file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token LegalDoc;
- appartiene a un lotto di documenti, a sua volta identificato univocamente nel sistema di conservazione;
- è conservato insieme al file delle direttive di conservazione, al file di ricevuta e al file di controllo del documento.

I documenti inviati nei formati standard, dettagliati nella documentazione contrattuale a disposizione del Cliente, sono visualizzabili mediante i relativi software definiti e messi a disposizione da InfoCert. Al momento dell'attivazione del servizio, il Cliente verifica che i documenti inviati siano nel formato standard leggibile con il software definito da InfoCert.

## 5.3 Configurazione dei sistemi

### 5.3.1 Modalità di erogazione

Il servizio di conservazione sostitutiva LegalDoc è implementato da una applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

LegalDoc è reso in modalità ASP (Application Service Providing) e consente al Cliente di accedere ai servizi di conservazione sostitutiva dei documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nel documento [1] *Condizioni Generali di Contratto* e nella relativa documentazione tecnica da questo referenziata.

Il servizio è accessibile dalla apposita URL di rete; il Cliente richiama i servizi di LegalDoc secondo le modalità indicate da InfoCert nella documentazione contrattuale.

Figura 1 offre uno schema esemplificativo del dialogo tra l'applicazione del Cliente e LegalDoc, distinguendo le parti che rimangono sotto la responsabilità del Cliente da quelle di competenza di InfoCert.

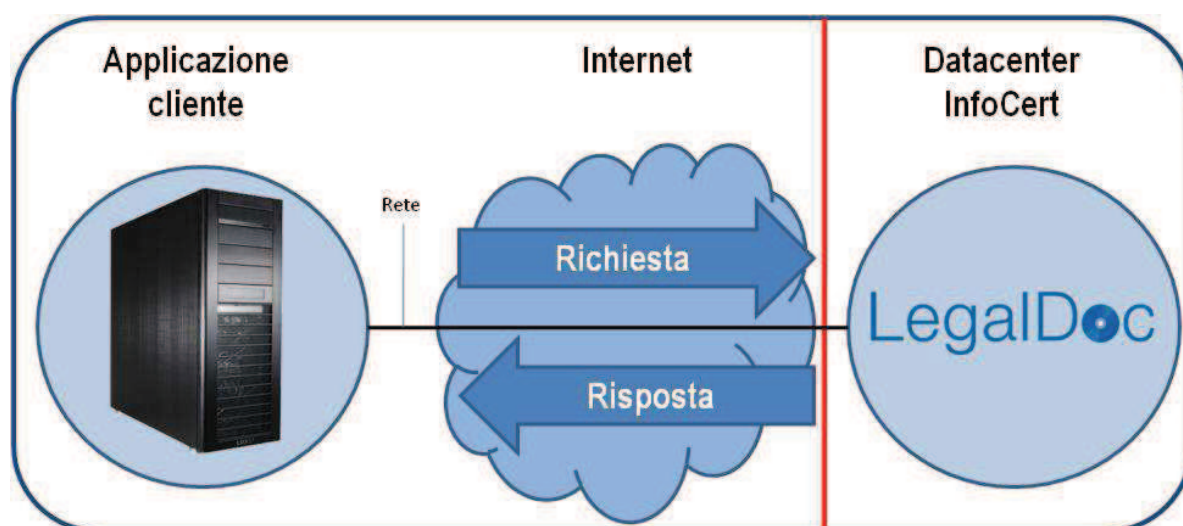


Figura 1 - Dialogo tra il sistema di gestione del Cliente e il sistema di conservazione documentale LegalDoc

## 5.4 Componenti

### 5.4.1 Marca temporale

Per l'emissione delle marche temporali LegalDoc si avvale del sistema di marcatura di InfoCert, Certification Authority accreditata. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert.

Il TSS è sincronizzato via radio con l'I.N.R.I.M di Torino (*Istituto Nazionale di Ricerca Metrologica*, già *Istituto Elettrotecnico Nazionale "Galileo Ferraris"*) ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

#### 5.4.2 Firma digitale con dispositivo HSM

Al buon esito del processo di conservazione, il Responsabile della Conservazione InfoCert appone la propria firma digitale sul file di chiusura lotto mediante un sistema di firma automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad alte prestazioni HSM.

#### 5.4.3 Supporti di conservazione

Ai fini della conservazione i documenti vengono raggruppati in lotti e ciascun lotto è corredato da un file indice (file di chiusura lotto) che contiene gli hash dei documenti appartenenti al lotto.

L'apposizione della firma digitale del RdC e della marca temporale sul file di chiusura lotto attestano la conservazione la conservazione del lotto.

I lotti prodotti vengono archiviati mediante procedure e sistemi che consentono la memorizzazione permanente in più copie e l'immodificabilità di quanto memorizzato.

Inoltre, possono essere prodotte ulteriori copie di back-up su supporti ottici rimovibili, stoccati da InfoCert o inviati al Cliente su espressa richiesta.

#### 5.4.4 Posta Elettronica Certificata

Il servizio LegalDoc si avvale del servizio PEC di InfoCert: in sede di attivazione del servizio, è stata definita per il Cliente una casella di posta certificata tramite la quale richiedere attività di supporto e inviare messaggi in genere alla casella di amministrazione [assistenza.legaldoc@legalmail.it](mailto:assistenza.legaldoc@legalmail.it).

### 5.5 Controlli

I processi del servizio di conservazione sostituiva LegalDoc sono fortemente automatizzati; i sistemi di erogazione sono dotati di molteplici funzioni di controllo in grado di rilevare e segnalare eventuali anomalie in essere o potenziali.

I controlli effettuati possono essere distinti secondo le seguenti tipologie:

- controlli di processo;
- controlli periodici.

#### 5.5.1 Controlli di processo

I controlli di processo sono i controlli che hanno luogo durante l'elaborazione dei documenti soggetti al processo di conservazione.

LegalDoc è un processo complesso che movimentata una consistente mole di dati, dei quali è necessario garantire costantemente l'integrità e la coerenza: per questo motivo sono attivati numerosi controlli automatici, che richiedono l'intervento del RdC solo al verificarsi di eventuali eventi anomali non gestibili in modo automatico.

Oltre a questi, le procedure di gestione del sistema prevedono un elenco di controlli manuali effettuati direttamente dal Responsabile della Conservazione o da un suo delegato.



### 5.5.2 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli di servizio per tutte le applicazioni.

La struttura si avvale di un gruppo di lavoro trasversale all'azienda e utilizza strumentazioni di varia natura per la raccolta di dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente per discutere dei malfunzionamenti registrati nel periodo e delle soluzioni adottate o potenziali per evitare il ripresentarsi dell'inconveniente

### 5.5.3 Ispezione del sistema da parte delle autorità competenti

In occasione delle ispezioni del sistema di conservazione da parte delle autorità competenti, gli esiti delle stesse e gli eventuali rilievi apposti sono registrati su appositi verbali.

Qualora dalle attività di ispezione e controllo emergessero punti critici o aree di miglioramento, è impegno di InfoCert l'attivazione delle strutture competenti per la tempestiva analisi della situazione e l'approntamento di tutte le misure necessarie al miglioramento del sistema e/o delle performance.

### 5.5.4 Incident management

InfoCert è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione documentale, al fine di individuare previamente ogni potenziale causa di incidente e provvedere alla sua rimozione, scongiurando il blocco del sistema o il danneggiamento dei file in esso contenuti.

I fornitori dei sistemi tecnologici utilizzati forniscono ad InfoCert tutte le opportune assicurazioni, rese per iscritto, contro il rischio di perdita dei documenti conservati.

Qualora si verificassero incidenti di sistema o di processo, le operazioni di ripristino della funzionalità seguono le procedure definite e documentate; per ogni incidente con impatti sul rispetto della normativa, è redatto un apposito verbale secondo la procedura definita.

Il Responsabile della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto di opportuni incontri di miglioramento.



## 6 Le tipologie documentali

### 6.1 Contratti

<b>Tipologia di documento</b>	Contratti
<b>Natura del documento</b>	Documento elettronico
<b>Conservabile in modalità elettronica</b>	Si
<b>Data di decorrenza del processo di conservazione elettronica</b>	dalla data di approvazione del presente Manuale

### 6.2 Atti Amministrativi

<b>Tipologia di documento</b>	Atti Amministrativi
<b>Natura del documento</b>	Documento elettronico
<b>Conservabile in modalità elettronica</b>	Si
<b>Data di decorrenza del processo di conservazione elettronica</b>	dalla data di approvazione del presente Manuale

I Contratti e gli Atti Amministrativi vengono creati mediante sistemi di videoscrittura in uso presso l'Ente in maniera statica e non modificabile (anche tramite l'applicativo gestionale Protocollo e Atti – Kibernetes srl); vengono poi firmati digitalmente da controparti e responsabili.

I documenti vengono poi inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale tramite una postazione pc, inserito nella rete intranet del Comune di Santa Giustina in Colle (PD)

### 6.3 Allegati

<b>Tipologia di documento</b>	Allegati a contratti e atti amministrativi
<b>Natura del documento</b>	Documento elettronico
<b>Conservabile in modalità elettronica</b>	Si
<b>Data di decorrenza del processo di conservazione elettronica</b>	Dalla data di approvazione del presente Manuale

## 6.4 Registro di protocollo

<b>Tipologia di documento</b>	Registro di protocollo
<b>Natura del documento</b>	Documento elettronico
<b>Conservabile in modalità elettronica</b>	Si
<b>Data di decorrenza del processo di conservazione elettronica</b>	Dalla data di approvazione del presente Manuale

Il Registro giornaliero di protocollo viene creato mediante sistema gestionale in uso presso l'Ente in maniera statica e non modificabile, viene firmato digitalmente dal Responsabile della gestione documentale o dal suo vicario ed inviato in conservazione sostitutiva a seguito caricamento manuale tramite una postazione pc collegata alla rete intranet del Comune di Santa Giustina in Colle (PD).

### 6.4.1 Fasi del processo

Contratti, Atti Amministrativi e loro allegati, Registro di Protocollo seguono il medesimo iter, per cui le fasi sono le stesse per tutte le tipologie documentali

<b>Fase / Attività</b>	<b>Soggetti incaricati</b>	<b>Afferenza / Applicativi</b>	<b>Descrizione</b>
<b>Redazione</b>	Utenti Ente	Sistemi di videoscrittura e pdf creator	Viene redatto il testo dell'atto, in formato elettronico
<b>Approvazione</b>	Organo competente	Firma digitale	L'atto viene approvato dall'organo competente, i cui componenti provvedono all'apposizione della propria firma digitale sul documento.
<b>Repertorizzazione</b>	Utenti Ente	Applicativo informatico e repertorio cartaceo presso Ufficio Segreteria/Contratti	Si provvede alla registrazione dell'atto utilizzando le funzionalità del sistema per registro determine, delibere, atti e protocollo; il Repertorio cartaceo per i Contratti fino all'attivazione del registro informatico
<b>Prelevamento dei documenti</b>	Ente: Referente di processo	I documenti vengono prelevati dall'apposita cartella creata nel server windows "Serverdati"	I documenti vengono inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale su interfaccia web tramite una postazione pc, inserita nella rete intranet del Comune di Santa Giustina in Colle (PD).

<b><i>Invio in conservazione</i></b>	Ente: Referente di processo	Legaldoc Folders (ora Legaldoc web)	Il sistema invia il documento in conservazione, richiedendo che il processo si concluda a riempimento dei lotti. È possibile richiedere la chiusura forzata del lotto
<b><i>Completamento del processo di conservazione</i></b>	InfoCert	LegalDoc	Il sistema di conservazione LegalDoc eroga il processo di conservazione dei documenti secondo quanto dettagliato al capitolo 7.
<b><i>Custodia dei supporti</i></b>	InfoCert	LegalDoc	La custodia dei supporti è demandata ad InfoCert come da accordi contrattuali

## 7 Il processo di conservazione

Il processo di conservazione attuato da InfoCert prevede l'utilizzo di diversi strumenti e l'intervento di soggetti che concorrono a rendere l'erogazione del servizio affidabile e rispondente ai requisiti richiesti dalla legge.

Ai fini del trattamento dei documenti destinati alla conservazione, il servizio si divide in due categorie di processi:

- processi di front-end;
- processi di back-end.

### 7.1 Processi di front-end

I processi di front-end sono erogati in modalità batch dal sistema LegalDoc Folders (ora LegalDoc web), e sono finalizzati a mettere in comunicazione i sistemi gestionali del Cliente con i servizi di LegalDoc e sono richiamati in modalità on-line.

Per ciascuno dei servizi indicati di seguito si eseguono opportuni controlli di autenticazione del soggetto chiamante e di correttezza e accettabilità delle richieste:

- invio di un documento informatico o di un documento analogico opportunamente digitalizzato in conservazione sostitutiva;
- rettifica o cancellazione per via telematica di un documento già conservato in modalità sostitutiva;
- esibizione di un documento direttamente dal sistema LegalDoc;
- elaborazione ed invio della richiesta di chiusura forzata del lotto;
- ottenimento per via telematica delle informazioni sullo stato di un documento o di un lotto.

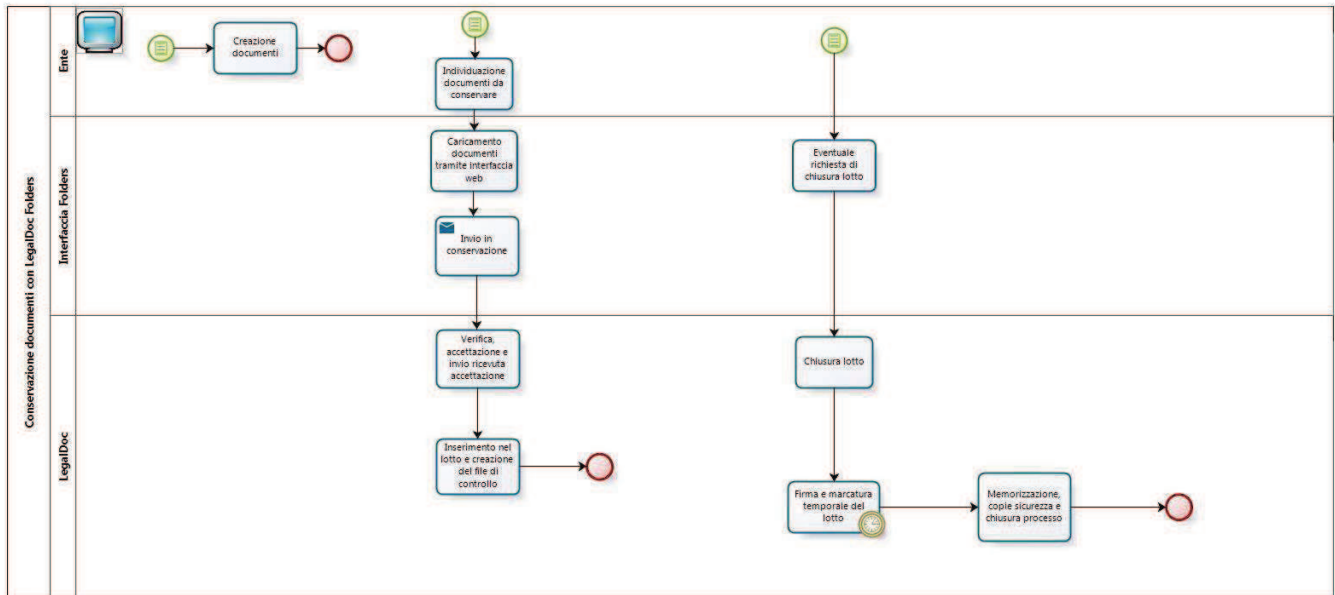
### 7.2 Processi di back-end

I processi di back-end sono eseguiti dal sistema LegalDoc in modalità differita e sono i processi che, a partire dai documenti caricati sul sistema LegalDoc Folders (ora LegalDoc web) dal Comune di Santa Giustina in Colle (PD) implementano la conservazione sostitutiva in conformità alle regole tecniche contenute nella deliberazione CNIPA 11/04.

Il processo di conservazione si suddivide in due macro fasi:

- **elaborazione del singolo documento:** in questa fase viene analizzato il singolo documento, che viene assegnato a un lotto di documenti. Il documento viene corredato da un file di controllo, firmato digitalmente dal Responsabile della Conservazione, contenente informazioni sensibili ai fini della conservazione (indice del documento, impronte dei file che lo costituiscono, classificazione anagrafica dei firmatari, lotto di appartenenza);
- **elaborazione e chiusura del lotto:** quando si raggiungono le condizioni per la chiusura del lotto, questo viene corredato da un file di chiusura lotto contenente informazioni sensibili ai fini della conservazione (identificativo univoco del lotto – tokenlotto –, criteri di omogeneità, hash del file di controllo). Al file di chiusura lotto viene apposta la firma digitale del Responsabile della Conservazione e la marca temporale; infine, l'insieme di documenti appartenenti al lotto, corredati dai rispettivi file di controllo e dal file di chiusura lotto, viene memorizzato nei supporti di conservazione e nelle copie di sicurezza.

### 7.3 Fasi del processo di conservazione: schema generale



### 7.4 Responsabilità del processo di conservazione

Nel processo di conservazione sostitutiva intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.



<i>Attività</i> ↗	<i>Responsabilità</i> ↗	<i>Comune di</i>	<i>LegalDoc Folders</i>	<i>LegalDoc</i>	<i>Responsabile della Conservazione</i>
1. Formazione del documento		<b>R - E</b>			
2. Indicizzazione e archiviazione		<b>R - E</b>			
3. Acquisizione documento e creazione del file con le direttive di conservazione		<b>V</b>	<b>R - E</b>		
4. Invio al sistema di conservazione		<b>R - E</b>	<b>R - E</b>		
5. Verifica e accettazione del documento e invio della ricevuta di accettazione dei documenti				<b>E - V</b>	
6. Inserimento nel lotto e creazione del file di controllo				<b>E</b>	<b>R - V* - A</b>
7. Chiusura del lotto e attestazione di corretto procedimento				<b>E</b>	<b>R - V* - A</b>
8. Memorizzazione, creazione "copia di sicurezza" e chiusura del processo				<b>E</b>	<b>R - V* - A</b>
[R-responsabile; E-esegue; V- verifica; A-approva]					

(\*)Tutte le verifiche in carico al Responsabile della Conservazione sono garantite anche dal servizio di auditing InfoCert.

## 7.5 Fasi del processo di conservazione: dettaglio

### 7.5.1 Formazione del documento

<i>INPUT</i>	<i>Documento da generare</i>	
<b>Comune di Santa Giustina in Colle (PD)</b>	1.1	Il Comune di Santa Giustina in Colle (PD) genera i documenti secondo le procedure descritte nel capitolo 4
<i>OUTPUT</i>	<i>Documento generato</i>	

### 7.5.2 Indicizzazione e archiviazione

<i>INPUT</i>	<i>Documento da archiviare</i>	
<b>Comune di Santa Giustina in Colle (PD)</b>	1.1	I documenti vengono inviati al sistema di conservazione sostitutiva a seguito del caricamento manuale su interfaccia web tramite una postazione pc, inserita nella rete intranet del Comune di Santa Giustina in Colle (PD)
<i>OUTPUT</i>	<i>Documento indicizzato e archiviato</i>	

### 7.5.3 Acquisizione documento e creazione del file delle direttive

<b>INPUT</b>	<i>File delle direttive da predisporre</i>	
<b>LegalDoc Folders</b>	2.1	Il sistema LegalDoc Folders acquisisce i documenti informatici caricati manualmente dal Comune di Santa Giustina in Colle (PD) e li prepara all'invio conservazione
<b>LegalDoc</b>	2.2	Il sistema LegalDoc esegue le seguenti operazioni: <ul style="list-style-type: none"> <li>• Predisposizione del file con le direttive di conservazione;</li> <li>• Calcolo delle impronte dei file costituenti il documento;</li> <li>• Inserimento delle impronte nel file delle direttive;</li> <li>• Apposizione della firma elettronica sul file delle direttive;</li> <li>• Costruzione del messaggio contenente i file che costituiscono il documento</li> </ul>
<b>OUTPUT</b>	<i>File delle direttive predisposto</i>	

### 7.5.4 Invio al sistema di conservazione

<b>INPUT</b>	<i>Documento da inviare a LegalDoc</i>	
<b>LegalDoc Folders</b>	3.1	Invoca i servizi di LegalDoc e invia il documento, il file degli indici di ricerca e la relativa richiesta di conservazione.
<b>OUTPUT</b>	<i>Documento inviato a LegalDoc</i>	

### 7.5.5 Verifica, accettazione e invio della ricevuta di accettazione del documento

<b>INPUT</b>	<i>Documento da verificare</i>	
<b>LegalDoc</b>	4.2	Acquisizione del documento.
	4.3	Sbustamento del messaggio e verifica della firma elettronica apposta sul file delle direttive di conservazione
	4.4	Presenza in carico dei file costituenti il documento.
	4.5	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione.
	4.6	Generazione dell'impronta di ogni file del documento.
	4.7	Confronto dell'impronta generata con la corrispondente inviata dal Cliente per garantire l'integrità del documento ricevuto.
<b>LegalDoc</b>	4.8	Nel caso di esito negativo delle verifiche, il documento viene respinto con l'indicazione che descrive l'errore intercorso. In questo caso il flusso termina.
	4.9	Generazione del file di ricevuta a partire dal file delle direttive.
	4.10	Generazione di un identificativo univoco per il documento (token LegalDoc) e firma elettronica sul file di ricevuta.
	4.11	Invio a LegalDoc Folders del file di ricevuta di presa in carico della richiesta di conservazione.

<b>LegalDoc Folders</b>	4.12	Riceve il file di ricevuta di presa in carico della richiesta di conservazione, ne estrae il token LegalDoc e lo memorizza presso i propri archivi, in associazione con gli indici di ricerca.
<b>OUTPUT</b>	<i>Documento verificato</i>	

### 7.5.6 Inserimento nel lotto e creazione del file di controllo

<b>INPUT</b>	<i>Documento da conservare</i>	
<b>LegalDoc</b>	5.1	Verifica per ogni documento se esiste già un lotto di documenti aperto che possiede le caratteristiche specificate dal file delle direttive in cui inserire il documento; in caso contrario si predispose un nuovo lotto.
	5.2	Predisposizione del file di controllo del documento contenente l'indice del documento, le impronte dei file che lo costituiscono, la classificazione anagrafica del documento, il lotto di appartenenza, gli estremi di identificazione del Responsabile della Conservazione.
	5.3	Apposizione della firma elettronica del Responsabile della Conservazione sul file di controllo.
	5.4	Inserimento del file di controllo e del relativo documento nel lotto di conservazione.
<b>OUTPUT</b>	<i>Documento inserito in un lotto di conservazione</i>	

### 7.5.7 Chiusura del lotto e attestazione di corretto procedimento

<b>INPUT</b>	<i>Lotto da chiudere</i>	
<b>LegalDoc</b>	7.1	Chiusura del lotto dopo il raggiungimento delle condizioni di chiusura lotto: <ul style="list-style-type: none"> <li>• raggiungimento della data massima di chiusura del lotto.</li> <li>• In base a criteri temporali definiti insieme al Comune di Santa Giustina in Colle (PD)</li> </ul> Il lotto viene chiuso al verificarsi del primo dei precedenti eventi o in seguito alla ricezione della richiesta di chiusura forzata del lotto inviata dal Cliente.
	7.2	Generazione del file di chiusura lotto e inserimento degli hash dei file di controllo del documento.
<b>Responsabile della Conservazione</b>	7.3	Apposizione della firma digitale, necessaria ad attestare il corretto svolgimento del procedimento sul file di chiusura lotto.
	7.4	Apposizione della marca temporale sul file di chiusura lotto.
<b>OUTPUT</b>	<i>Lotto chiuso</i>	

### 7.5.8 Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

<b>INPUT</b>	<i>Documenti da memorizzare</i>	
<b>LegalDoc</b>	8.1	Memorizzazione del lotto su supporto magnetico.
	8.2	Creazione della copia di sicurezza.



	8.3	Termine della procedura di conservazione.
OUTPUT	<i>Documenti conservati</i>	

## 8 Procedure di ricerca ed esibizione

Le procedure di esibizione del documento integrate in LegalDoc permettono, a partire dalla funzione di ricerca in LegalDoc Folders, di estrarre dal sistema un documento di cui sia completata la procedura di conservazione, utilizzando il token LegalDoc.

L'esibitore è un'applicazione in tecnologia web, che permette ad un utente, precedentemente definito e in possesso delle debite autorizzazioni e credenziali, di accedere al sistema di conservazione LegalDoc da una qualsiasi stazione di lavoro (computer), purché collegata in rete e con disponibilità di un browser web.

L'interfaccia è organizzata a schede, ognuna delle quali tratta un aspetto relativo alla conservazione del documento.

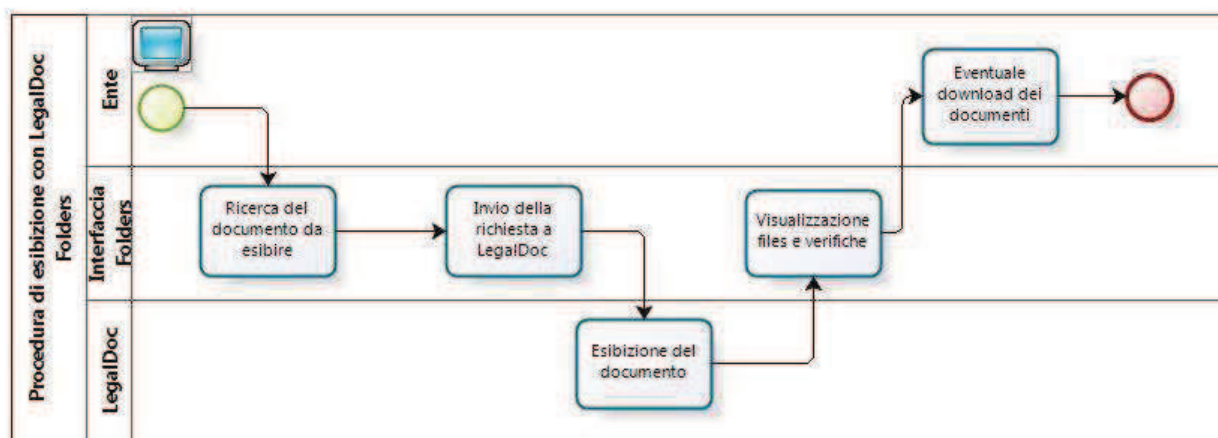
Visualizzando il contenuto di ciascuna scheda diventa possibile:

- estrarre un documento e visualizzarlo a video
- produrre copia cartacea o su altro supporto informatico del documento
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione
- prendere visione dei file a corredo che qualificano il processo di conservazione attestandone il corretto svolgimento
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione
- verificare l'integrità del documento

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 6 della deliberazione CNIPA 11/04.

Di seguito si descrivono le fasi della procedura di ricerca ed esibizione.

### 8.1 Procedura di esibizione: schema generale





## 8.2 Procedura di esibizione: dettaglio

### 8.2.1 Ricerca del documento da esibire

<b>INPUT</b>	<i>Lista di documenti</i>	
<b>Comune di Santa Giustina in Colle</b>	1.1	Attraverso LegalDoc Folders (ora LegalDoc web) utilizzando gli indici archiviati nel proprio gestore documentale, ricerca il documento da esibire
	<b>OUTPUT</b> <i>Token relativo al documento da esibire</i>	

### 8.2.2 Invio della richiesta a LegalDoc

<b>INPUT</b>	<i>Richiesta di esibizione da preparare</i>	
<b>LegalDoc Folders</b>	2.1	LegalDoc Folders seleziona il token relativo al documento da esibire.
	2.2	Creazione del file delle direttive di esibizione, contenente il token LegalDoc relativo al documento da esibire, e sua sottoscrizione digitale.
	2.3	Chiamata al servizio LegalDoc.
<b>OUTPUT</b>	<i>Richiesta di esibizione presa in carico da LegalDoc</i>	

### 8.2.3 Ricerca del documento nel sistema ed esibizione

<b>INPUT</b>	<i>Richiesta di esibizione acquisita</i>	
<b>LegalDoc</b>	3.1	Ricezione della richiesta di esibizione del documento.
	3.2	Controllo di corrispondenza tra il token LegalDoc inviato dal Cliente e quelli dei documenti conservati.
	3.3	Predisposizione delle copie di: <ul style="list-style-type: none"> <li>• file costituenti il documento conservato</li> <li>• file di ricevuta</li> <li>• file di controllo del documento.</li> </ul>
	3.4	Passaggio del pacchetto di file all'Esibitore
<b>OUTPUT</b>	<i>Documento passato all'Esibitore</i>	

### 8.2.4 Verifica del documento

<b>INPUT</b>	<i>Documento ricevuto dal sistema di conservazione</i>	
<b>Esibitore</b>	4.1	Visualizzazione del pacchetto di file ed effettuazione di tutte le verifiche.
<b>OUTPUT</b>	<i>Documento esibito</i>	

### 8.2.5 Verifica del documento

<i>INPUT</i>	<i>Documento esibito</i>	
<b>Esibitore</b>	5.1	Download del documento e memorizzazione dello stesso in locale
<i>OUTPUT</i>	<i>Documento salvato</i>	

### 8.3 Requisiti software

Per la visualizzazione e la stampa del documento ottenuto con la procedura di esibizione da LegalDoc, il Comune di Santa Giustina in Colle (PD) utilizza, per ognuno dei file costituenti il documento, il relativo viewer definito da InfoCert per i formati standard o depositato presso il sistema di conservazione per le altre tipologie di file.



## 9 Modifica dei documenti posti in conservazione

In caso di modifica dei documenti già posti in conservazione, il Comune di Santa Giustina in Colle (PD) provvede ad emanare ex novo un documento di rettifica che verrà a sua volta conservato a norma; la riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti dal Comune di Santa Giustina in Colle (PD) in fase di caricamento, che ne assicura la sistematicità e la coerenza.

### 9.1 La cancellazione di un documento

LegalDoc è configurato in modo da non consentire la cancellazione fisica di quanto conservato: il servizio di cancellazione consiste nella cancellazione logica del documento dal database.

La cancellazione può essere richiesta solo dal sistema di interfaccia a LegalDoc che ha fatto la richiesta di invio in conservazione del documento da cancellare.

## 10 Misure di sicurezza

### 10.1 Comune di Santa Giustina in Colle (PD)

Per le misure di sicurezza nel trattamento dei documenti del Comune di Santa Giustina in Colle (PD) si rimanda alla procedure vigenti da esso predisposto.

### 10.2 InfoCert

Il sistema LegalDoc è pienamente conforme ai requisiti di sicurezza prescritti dalle norme. Nel seguito sono descritte le modalità generali tecniche e le infrastrutture che InfoCert utilizza all'interno del proprio data center di Padova, in quanto fornitore del servizio di conservazione.

#### 10.2.1 Sicurezza fisica

I locali che ospitano il sistema LegalDoc sono in un immobile la cui zona d'ubicazione non presenta rischi ambientali dovuti alla vicinanza ad installazioni pericolose. Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica. Per questi locali sono presenti le apparecchiature e gli accessori di controllo e di sicurezza previsti dalle norme in vigore. Lo stabile è inoltre sorvegliato da personale specializzato 24 ore al giorno.

La sala CED è l'area protetta all'interno dello stabile, accessibile mediante utilizzo del badge autorizzato, dove si trovano i dispositivi hardware e software dei diversi sistemi InfoCert.

L'accesso alla sala CED è consentito solamente alle persone autorizzate, ossia quelle con un ruolo operativo nell'erogazione del servizio e nella gestione dell'infrastruttura.

All'interno della sala CED sono collocate le sale denominate locale CA, accessibili mediante badge autorizzato e PIN (Personal Identification Number) di accesso. L'accesso ai singoli locali del locale CA necessita di un ulteriore badge autorizzato.

La sala CED è dotata di telecamere a circuito chiuso, rilevatori combinati microonde e infrarossi, rilevatori ottici di fumo sul soffitto e nel sottopavimento, avvisatori manuali di allarme, avvisatori ottici acustici d'allarme per avviso locale, sensori piezodinamici per la rilevazione della rottura dei vetri. Tutte le porte sono dotate di allarme.

#### 10.2.2 Gruppi di continuità

Tutte le apparecchiature del centro dati di InfoCert a Padova sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso di interruzione dell'energia elettrica da parte del fornitore. In caso di assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

#### 10.2.3 Connessione a Internet

Il centro dati di InfoCert è connesso alla rete Internet con due collegamenti ATM separati, entrambi con velocità massima di 155 Mbit/sec.

Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati di interfaccia separati e completamente ridondati.

InfoCert è impegnata a mantenere tempi di attraversamento rete inferiori a 20 ms tra il proprio Centro Servizi e i nodi d'interconnessione con i principali provider italiani e internazionali.

#### 10.2.4 Sicurezza delle reti: protezione da intrusioni

I sistemi e le reti di InfoCert sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (DeMilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite.

Le regole definite sui firewall vengono progettate in base a due principi: in primis il “default deny”, ossia quanto non è espressamente permesso è vietato di default ed è, quindi, consentito solo quanto è strettamente necessario al corretto funzionamento dell'applicazione. Il secondo principio consiste nel “defense in depth”, secondo il quale vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, poi a livello di sistema (hardening).

InfoCert provvede alla gestione e all'implementazione delle regole di sicurezza dei firewall. I sistemi firewall sono configurati in alta affidabilità (HA), ovvero sono formati da coppie di macchine indipendenti, collegate tra loro e gestite tramite appositi software in modo che, in caso di guasto di una delle macchine, il traffico venga dirottato sulla macchina di backup.



## 11 Note conclusive

### 11.1 Procedure di riversamento

#### 11.1.1 Riversamento diretto

Il primo comma, lettera n., dell'articolo 1 della deliberazione CNIPA 11/2004 definisce il riversamento diretto come il "processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica".

Le norme non pongono particolari obblighi nello svolgimento del processo, che è parte integrante del servizio.

#### 11.1.2 Riversamento sostitutivo

Qualora fosse necessario, o in presenza di una espressa richiesta del Comune di Santa Giustina in Colle (PD), il Responsabile della Conservazione InfoCert provvede al riversamento sostitutivo del contenuto dei supporti, inteso come il "processo che trasferisce uno o più documenti informatici conservati da un supporto ottico ad un altro, modificando la loro rappresentazione informatica" (deliberazione CNIPA 11/2004, articolo 1 comma 1 lettera o.).

Alla data di redazione del presente documento non sono riscontrabili motivazioni tecnologiche, legali o di altra natura che impongano o possano richiedere nei prossimi anni l'effettuazione del riversamento sostitutivo e la conseguente conversione dei documenti conservati in altri con differente rappresentazione informatica.

I controlli periodici messi in atto dal Responsabile della Conservazione InfoCert permettono di monitorare costantemente l'evoluzione dei diversi scenari di riferimento (tecnologico, normativo...) al fine di rispondere all'esigenza di riversamento sostitutivo dei documenti conservati non appena questa dovesse manifestarsi.

Il riversamento sostitutivo verrà effettuato secondo procedure che saranno definite e documentate al bisogno, in relazione al futuro scenario normativo e tecnologico di riferimento.

### 11.2 Protezione dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione della documentazione cartacea e elettronica, il Comune di Santa Giustina in Colle (PD) pone la massima cura nel rispetto delle disposizioni stabilite dal D.Lgs n. 196/2003 "Codice in materia di protezione dei dati personali".

Ai sensi dell'articolo 29 Codice, il Comune di Santa Giustina in Colle (PD) ha nominato InfoCert SpA Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio (allegato [2]).

In particolare, anche in considerazione del ruolo di Responsabile della Conservazione ricoperto, i compiti affidati ad InfoCert SpA attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati.

InfoCert opera quale Responsabile del trattamento applicando le misure di sicurezza in base alle disposizioni legislative e regolamentari in vigore.

L'informativa di cui all'articolo 13 del D.Lgs. 196/2003 per i dati relativi al contratto è resa al Comune in allegato al materiale contrattuale da questi sottoscritto, ove viene altresì allo stesso consentito di esprimere il consenso per gli ulteriori trattamenti indicati.



## 12 Allegati

### 12.1 Documentazione contrattuale di riferimento

Si fornisce di seguito un elenco dei documenti contrattuali a cui il Manuale si riferisce.

I documenti sotto riportati si intendono come riferimenti ufficiali: eventuali discrepanze fra quanto indicato nel Manuale e quanto presente nei documenti presenti nel seguente elenco si risolvono in favore di questi ultimi.

- [1] Richiesta di attivazione con Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e Comune di Santa Giustina in Colle (PD);
- [2] Affidamento del procedimento di conservazione sostitutiva – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;
- [3] Allegato Tecnico al contratto – descrive le modalità di fornitura del servizio e l'infrastruttura utilizzata per la sua erogazione.
- [4] Allegato Tecnico del 22/09/2015 – Descrive la configurazione Legaldoc con l'integrazione della classe "Registro di protocollo"



**Allegato contrattuale**  
**AL - Servizio LegalDoc Folders**



## Indice generale

<b>1. Introduzione al documento.....</b>	<b>3</b>
1.1 Scopo e campo di applicazione del documento.....	3
1.2 Riferimenti.....	3
<b>2. Il servizio.....</b>	<b>4</b>
2.1 Caratteristiche del servizio.....	4
2.1.1 Disponibilità dei dati.....	5
2.2 Precisazioni.....	6
2.3 Utilizzo del servizio di posta elettronica integrata (opzionale).....	6
2.4 Utilizzo del servizio di firma automatica da remoto (opzionale).....	6
2.5 Utilizzo del servizio di marcatura temporale (opzionale).....	6
2.6 Formazione del Libro Unico del Lavoro (opzionale).....	7
2.7 Integrazione funzionale sulle modalità di conservazione.....	7
<b>3. Supporto.....</b>	<b>9</b>
<b>4. Accesso al servizio.....</b>	<b>10</b>
4.1 Prerequisiti.....	10
4.1.1 Hardware.....	10
4.1.2 Software.....	10
4.1.3 Browser.....	10
4.1.4 Connettività.....	10
4.2 Strumenti di identificazione.....	10
<b>5. Livelli di servizio.....</b>	<b>11</b>
5.1 Modalità di erogazione.....	11
5.2 Service Level Agreement.....	12
5.3 Criteri di misurazione.....	12
<b>6. Allegato.....</b>	<b>14</b>
6.1 Informazioni sul Data Center.....	14

## **1.Introduzione al documento**

Il presente documento costituisce l'Allegato alle Condizioni Generali del Contratto per l'uso del servizio LegalDoc Folders in modalità A.S.P.

Il Servizio LegalDoc Folders è reso in modalità A.S.P. (*Application Service Providing*) e consente al Cliente di accedere ai servizi di conservazione sostitutiva dei propri documenti informatici su un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima.

LegalDoc Folders è un servizio per la conservazione sostitutiva e l'esibizione di documenti informatici in ottemperanza a:

- Decreto Ministero delle Entrate e delle Finanze 23 gennaio 2004, modificato dal Decreto Ministero dell'Economia e delle Finanze 06/03/2009
- Deliberazione CNIPA n. 11/2004: regole tecniche per la riproduzione e conservazione su supporto idoneo a garantire la conformità dei documenti agli originali
- Decreto Legislativo 52/2004

Il Servizio è accessibile dall'apposita URL di rete: <http://ldocfolders.infocert.it>

### **1.1 Scopo e campo di applicazione del documento**

Il documento ha l'obiettivo di descrivere il contenuto, le modalità di erogazione, le condizioni d'accesso, le caratteristiche del servizio.

Di seguito vengono elencati i richiami presenti nella documentazione contrattuale verso il presente allegato.

<i>Contratto</i>	<i>Allegato</i>
Definizioni	Spiegazioni
Art. 1.3 Caratteristiche del Servizio	Cap. 2.2 Caratteristiche principali del servizio Cap. 2.3 Ulteriori condizioni del servizio
Art. 1.6 Supporto	Cap. 3 Supporto
Art. 1.8 Obblighi del cliente	Cap. 4 Accesso al servizio [1] MO – Specifiche tecniche di collegamento
Art. 1.9 Obblighi di InfoCert	[1] MO – Specifiche tecniche di collegamento
Art. 2.1 Livelli di servizio	Cap. 5 Livelli di servizio
Art. 2.2 Requisiti hardware e software	Cap. 4.1 Prerequisiti
Art. 2.3 Connettività	Cap. 4.1.3 Connettività
Art. 3.1 Identificativi ed accessi al sistema	Cap. 4.2 Strumenti di identificazione
Art. 3.4 Conservazione dei dati	Cap. 2.2.1 Disponibilità dei dati

### **1.2 Riferimenti**

- [1] MO – LegalDoc Folders - Specifiche tecniche generali
- [2] MU/LDOC – Manuale utente conservazione sostitutiva LegalDoc
- [3] SPT/LDOC – Specifiche Tecniche di integrazione LegalDoc
- [4] SPT/TAPE - LegalDoc Connector - Specifiche tecniche di collegamento



## **2. Il servizio**

La conservazione sostitutiva dei documenti, secondo le regole tecniche emanate con la deliberazione *CNIPA n° 11/2004* e con il *Decreto del Ministero Economia e Finanze del 23 gennaio 2004 e successive modifiche*, rappresenta una concreta opportunità di cost-saving per Imprese, Professionisti e Pubbliche Amministrazioni.

La *deliberazione CNIPA n° 11/2004* fissa le regole che consentono di sostituire i documenti cartacei con documenti informatici, mediante la memorizzazione di questi ultimi su un supporto informatico idoneo a garantirne la conformità agli originali; precisa inoltre le modalità tecniche per la conservazione dei “documenti informatici” con piena validità legale.

Il *DMEF 23 gennaio 2004* stabilisce le modalità per la conservazione e la riproduzione delle scritture e dei documenti contabili su supporti informatici, con effetto anche ai fini fiscali e con la conseguente possibilità di sostituire gli archivi cartacei e di conservare fatture trasmesse in forma elettronica e secondo le regole prescritte dal *Dlgs n° 52 del 20 febbraio 2004* (che ha recepito la *Direttiva comunitaria n° 2001/115/CE*).

### **2.1 Caratteristiche del servizio**

Il servizio è realizzato con tecnologia web-based ed è erogato in modalità ASP da InfoCert, secondo uno schema di Business Process Outsourcing (BPO). Prevede i servizi di seguito elencati:

- Funzioni minime di Gestione Documentale
- Conservazione sostitutiva (comprensiva del servizio di firma digitale e marcatura temporale)
- Gestione integrata di userid e password per l'accesso all'applicazione
- Invio automatico dei documenti via Posta Elettronica Certificata (opzionale)
- Servizio di firma massiva da remoto (opzionale)
- Servizio di marcatura temporale (opzionale)

#### **Schema funzionale per la fattura (esemplificazione)**

Il modello prevede due possibilità di trasmissione del documento fattura: massiva (tramite caricamento automatico) oppure manuale (ovvero online, mediante caricamento su web-form).

Una volta controllate, le fatture sono inviate al Sistema di Conservazione Sostitutiva, e al termine del procedimento diventano disponibili per l'esibizione e la ricerca.

#### **Schema funzionale per altri documenti (contabili, amministrativi, legali, dichiarativi,...)**

La validità dello schema funzionale appena descritto, per i fini dell'archiviazione e della conservazione, è replicato anche a tutti gli altri tipi di documento gestiti dal servizio.

#### **Conservazione sostitutiva**

Per la conservazione sostitutiva a norma dei documenti, il modello HUB utilizza un sistema integrato di procedure e tecnologie che ne garantisce **integrità, autenticità, riservatezza e disponibilità** nel tempo, nel pieno rispetto della normativa vigente.

Il sistema utilizzato garantisce:

- la conservazione sostitutiva di documenti informatici su adeguati supporti;
- la firma digitale e la validazione temporale serializzate di insiemi di documenti informatici;

- l'esibizione, per via telematica, di un documento conservato in modalità sostitutiva;
- l'organizzazione e la classificazione dei documenti conservati per insiemi omogenei e parametri permanenti di ricerca;

Il procedimento di conservazione digitale è affidato alla sicurezza dei sistemi ed alla competenza degli specialisti di InfoCert, cui sono delegate anche le incombenze previste dalla legge per il **Responsabile della Conservazione**.

Per ulteriori informazioni si veda la documentazione LegalDoc [2].

#### **Sicurezza ed affidabilità del Sito InfoCert**

- Sistemi di sicurezza anti-intrusione
- Società certificata ISO – 9000 dal marzo 1999
- Certificatore accreditato DigitPA dal 19 luglio 2007

#### **Eterogeneità e flessibilità della fase di Acquisizione**

- Modalità di inoltro del documento sia online (via web), sia in differita (solo modalità massiva) come indicato in [1]
- Flussi di acquisizione nei formati indicati nella Scheda A- Dati Tecnici di Attivazione
- Conservazione a norma CNIPA 11/2004
- DMEF 23 gennaio 2004

#### **Funzionalità di ricerca e consultazione**

- Ricerca secondo i parametri fissati dal DMEF 23 gennaio 2004
- Esibizione dei documenti conservati

#### **2.1.1 Disponibilità dei dati**

InfoCert provvede a concludere il processo di conservazione dei documenti inviati non appena si verifica una delle condizioni definite nei successivi paragrafi.

Alla ricezione dei documenti, mediante modalità massiva tramite lo strumento LegalDoc Connector, viene prodotta una distinta, notificata al cliente mediante messaggio di posta elettronica certificata (PEC) (per approfondimenti cfr. [1]).

Per i documenti che lo necessitano viene mantenuto l'ordine cronologico nelle modalità descritte in [1].

Su richiesta del cliente, è possibile attivare un controllo di sequenzialità della numerazione dei documenti, rilevando eventuali MANCANZE di numerazione. In tal caso la componente LegalDoc Connector impedisce l'invio dei documenti in conservazione sino a che l'anomalia non sia sanata.

La componente LegalDoc Connector esegue il controllo preventivo sulla qualità dei dati inviati in conservazione e **ne impedisce l'invio qualora riscontri delle anomalie**.

Nell'eventualità che uno o più documenti non superino i controlli definiti in [1] e [4], al Cliente viene notificata la presenza di errori attraverso un messaggio di posta elettronica certificata. **E' compito del Cliente porre rimedio alle anomalie segnalate prima di ritentare la trasmissione.**

### **Archivio di deposito**

I documenti caricati, per i quali non si sia ancora chiuso il processo di conservazione, rimangono depositati all'interno delle aree private del servizio (archivio di deposito) e non sono accessibili tramite l'esibizione a norma, bensì tramite l'erogazione (consultazione non a norma).

Sono visualizzati con la dicitura "In Lavorazione".

I documenti inseriti nell'archivio di deposito sono disponibili per l'erogazione dal momento della ricezione nel sistema di conservazione LegalDoc per il tempo necessario alla chiusura del di conservazione. L'operazione di erogazione è considerata, ai fini dei consumi, come un'esibizione a norma.

### **2.2 Precisazioni**

Il servizio LegalDoc Folders non permette:

- non è permesso al Cliente di autogenerare fatture (D.Lvo 52/2004)
- DMEF 23 gennaio 2004 art. 5: non è generata l'impronta dell'archivio in attesa delle specifiche tecniche che dovranno essere emanate da parte dell'Agenzia delle Entrate

### **2.3 Utilizzo del servizio di posta elettronica integrata (opzionale)**

#### **Posta elettronica e/o posta elettronica certificata**

Il Cliente ha la possibilità di richiedere la configurazione di una casella di posta elettronica certificata al fine di trasmettere, in modo automatico, le fatture elettroniche o altri documenti gestiti dal servizio LegalDoc Folders ad una serie di destinatari dallo stesso predefiniti all'interno del servizio.

E' responsabilità del Cliente, pertanto, definire correttamente gli indirizzi di posta elettronica dei destinatari all'interno dell'applicazione.

Sarà completa cura del Cliente, altresì, la gestione della casella di posta elettronica in dotazione (ricezione avvisi di consegna e/o mancato recapito, conservazione delle ricevute, verifica spazio disponibile, etc.).

Per l'utilizzo di posta elettronica certificata il Cliente prende atto dell'applicazione delle relative norme di legge, ed, in particolare, del D.P.R. n. 68/2005 e delle regole tecniche di cui al D.M. 2.11.2005 e delle relative condizioni di servizio InfoCert.

### **2.4 Utilizzo del servizio di firma automatica da remoto (opzionale)**

Il Cliente ha la possibilità di richiedere l'attivazione, all'interno dell'applicazione LegalDoc Folders, del servizio di firma automatica da remoto dei documenti rilevanti ai fini tributari.

La soluzione permette di apporre tramite LegalDoc Folders un numero elevato di firme gestendo da remoto (in termini di attivazione/disattivazione) il certificato di firma utilizzato per la sottoscrizione, secondo le relative condizioni del servizio InfoCert.

### **2.5 Utilizzo del servizio di marcatura temporale (opzionale)**

Il Cliente ha la possibilità di richiedere l'attivazione, all'interno della applicazione LegalDoc Folders, del servizio InfoCert di marcatura temporale. Il cliente può richiedere l'applicazione della marca temporale su tutti i documenti di una o più classi documentali; InfoCert provvede alla

marcatura temporale contestualmente alla firma digitale dei documenti prima del loro invio in conservazione, secondo le relative condizioni del servizio InfoCert.

## **2.6 Formazione del Libro Unico del Lavoro (opzionale)**

Nel caso di adozione del servizio di formazione del Libro Unico del Lavoro, ai sensi dell'art. 1.8 "Obblighi del Cliente" e 4.1. "Responsabilità del Cliente" delle condizioni generali di contratto, il Cliente prende atto che:

- qualora l'apposizione del numero di pagina sui documenti che costituiscono il Libro Unico del Lavoro avvenga autonomamente per opera del Cliente e/o comunque non dipenda da azioni di InfoCert la stessa è sollevata da ogni e qualsiasi responsabilità in merito alla numerazione e sequenzialità dei predetti documenti;
- qualora l'apposizione del numero di pagina sui documenti che costituiscono il Libro Unico del Lavoro avvenga da parte di InfoCert quest'ultima garantisce unicamente la sequenzialità della numerazione.

## **2.7 Integrazione funzionale sulle modalità di conservazione**

Per tutti i documenti avviati alla conservazione in modalità massiva si può specificare la data massima di conservazione nelle modalità descritte [1] e [4]. Se presente, questo parametro regola la chiusura del processo di conservazione e LegalDoc Folders garantisce la chiusura del processo di conservazione entro tale data a prescindere da tutti gli altri parametri di configurazione. La data massima di conservazione **deve essere sempre almeno 3 giorni successiva** alla data di invio in conservazione.

Nel caso di documentazione fiscale, in cui il termine del processo di conservazione è vincolato dalle normative di riferimento, se il cliente non valorizza la data massima di conservazione il sistema imporrà la conservazione in modo da rispettare le disposizioni di legge in base alla tipologia documentale oggetto della conservazione, specificata dal Cliente stesso.

In tutti gli altri casi in cui quanto sopra non sia applicabile, ad esempio nel caso in cui il Cliente abbia inviato i documenti non rispettando gli SLA contrattuali, il sistema impone la prima data utile accettata dal motore di conservazione LegalDoc (ovvero il giorno successivo rispetto l'istante di elaborazione).

I termini della conservazione sono impostati sul tipo documento agendo sulla combinazione: **periodo di chiusura (PdC) e termine limite di conservazione (TL)** (definiti in fase contrattuale).

Questi sono da intendersi come ulteriori parametri di chiusura, rispetto alla data massima di conservazione.

Per la documentazione di natura fiscale questi parametri vanno configurati secondo le disposizioni normative vigenti.

Per i documenti di natura non strettamente fiscale, o in generale non soggetti a disposizione di legge, i termini sono concordati fra il Cliente e InfoCert in fase contrattuale.

Il "periodo di chiusura" specifica il tempo, in giorni solari, entro il quale si chiude il processo di conservazione. L'intervallo di tempo è calcolato a partire dalla **data del documento** (parametro obbligatorio da indicare tra i dati indice del documento).

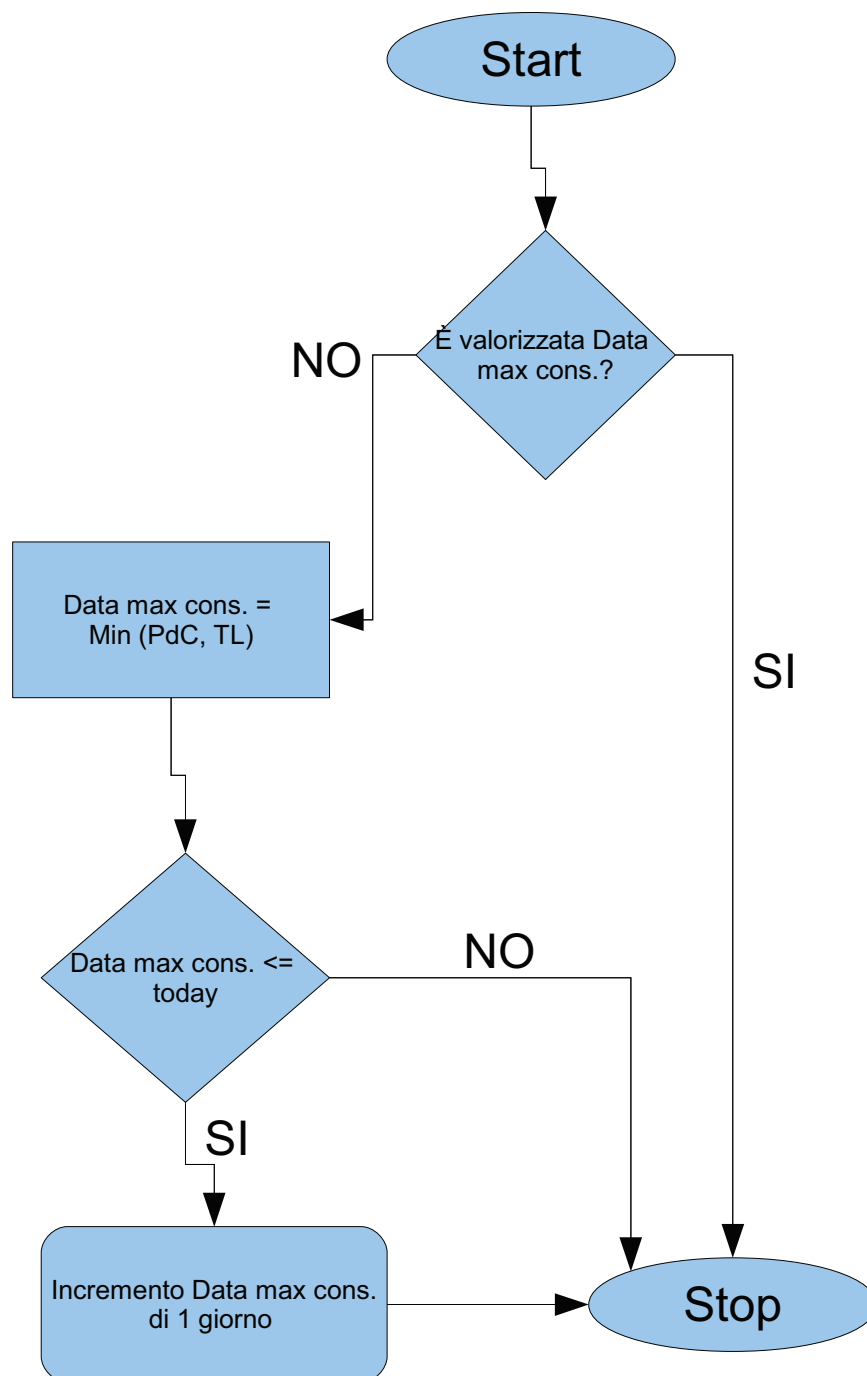
Il "termine limite" stabilisce in modo preciso una data entro la quale conservare.

Vediamo con un esempio come agisce in pratica il combinato predisposto:

- si stabilisce il periodo di chiusura PdC a 45 gg
- si fissa il termine limite TL al 31 dicembre

Un documento avente data 2 aprile verrà conservato entro il 16 maggio (2 aprile + PdC) e così via a seguire per tutti i documenti della stessa categoria. Nel caso in cui il documento sia inviato abbia data 2 dicembre, senza il TL, verrebbe chiuso il 15 gennaio ma nel caso il cliente ritenga di organizzare la conservazione per anno, la valorizzazione di TL comporterà una chiusura anticipata rispetto ai termini.

Il seguente diagramma specifica in dettaglio l'algoritmo utilizzato:





Nel caso i parametri periodo di chiusura e tempo limite non siano presenti, non viene impostata alcuna data massima di conservazione e la chiusura dei lotti avverrà secondo le regole del sistema di conservazione LegalDoc (cfr. [3]).

### **3.Supporto**

Il Customer Care è a disposizione al numero telefonico: **199.500.130**

L'assistenza coprirà i seguenti orari:

lunedì -venerdì dalle 08.00 alle 19.00, eccetto festivi

sabato dalle 08.00 alle 14.00, eccetto festivi

Durante la fase di attivazione, per tutte le problematiche di natura tecnica relativa all'integrazione, si potrà contattare la casella e-mail di assistenza tecnica [postvendita@infocert.it](mailto:postvendita@infocert.it)

## **4. Accesso al servizio**

### **4.1 Prerequisiti**

I requisiti per accedere al Servizio sono:

- essere titolari di una casella di posta elettronica certificata, dove il Cliente riceverà tutte le comunicazioni di servizio da InfoCert
- possedere gli strumenti tecnici necessari (hardware, software e collegamenti telematici) per il collegamento all'URL dove risiede il Servizio;
- avere affidato lo svolgimento delle attività del procedimento di conservazione ad InfoCert a norma dell'Art. 5, Comma 3 della citata Delibera CNIPA n. 11/2004
- fornire ad InfoCert tutte le informazioni richieste, necessarie alla configurazione del sistema
- verificare la congruità dei viewer standard proposti da InfoCert per la lettura dei documenti conservati o depositare, presso InfoCert, appositi visualizzatori

L'accesso avviene tramite collegamento sicuro all'URL <http://ldocfolders.infocert.it>

La trasmissione massiva di documenti avviene tramite la componente LegalDoc Connector (<http://legaldocconnector.infocert.it>)

#### **4.1.1 Hardware**

Le Piattaforme previste dalla componente software LegalDoc Connector client, sono descritte in [4]

#### **4.1.2 Software**

I documenti sono conservati con i visualizzatori predefiniti da InfoCert.

#### **4.1.3 Browser**

Microsoft Internet Explorer v. 7.0 o superiori

#### **4.1.4 Connettività**

Connessione effettuata tramite collegamento ad Internet di qualsiasi tipo. Le performances (tempi di risposta) del servizio dipendono fortemente dalla tipologia di connettività scelta.

## **4.2 Strumenti di identificazione**

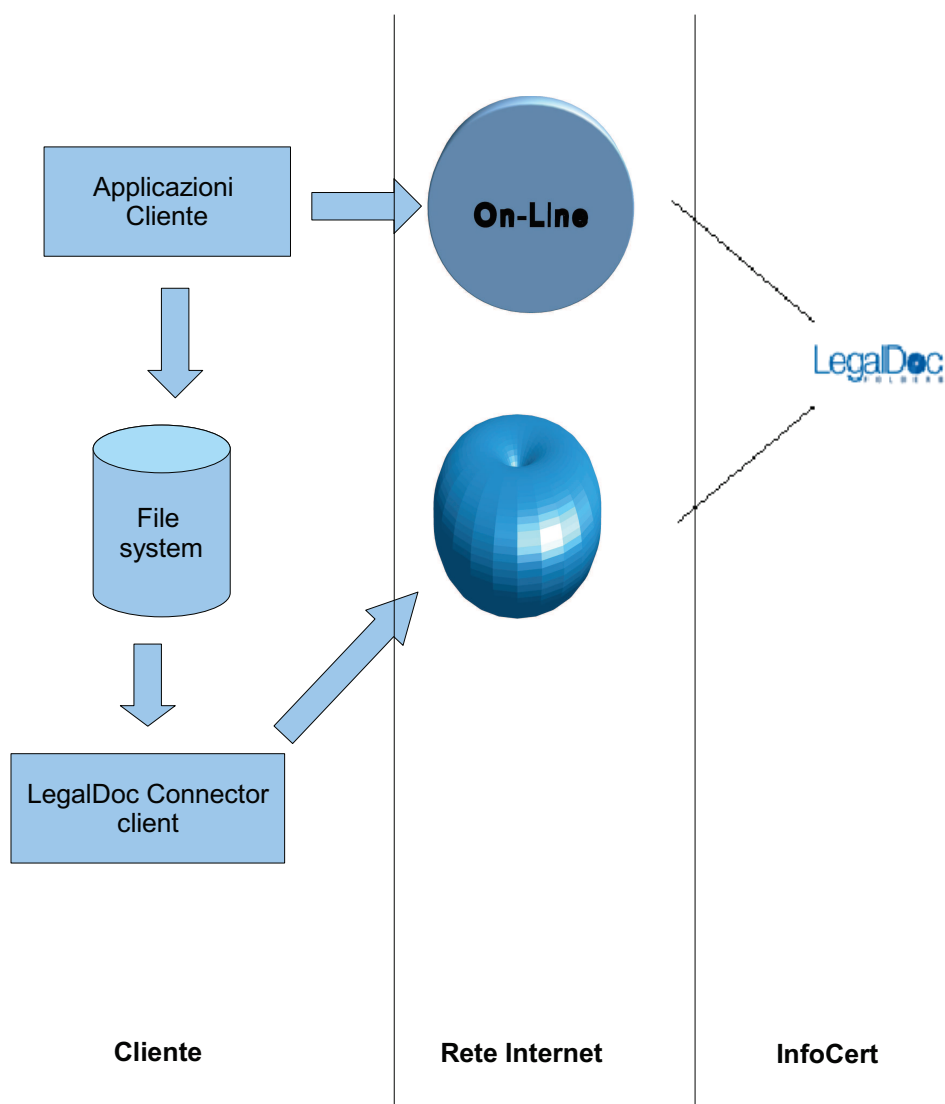
Gli strumenti per accedere al Servizio sono una coppia di user e password per l'accesso online per richiedere in esibizione i documenti conservati e per l'utilizzo della componente LegalDoc Connector. In seguito all'esito positivo della procedura di identificazione tutte le operazioni si considerano effettuate dal Cliente, il quale è obbligato ad osservare la massima diligenza nell'utilizzo, conservazione e protezione di tale identificativo e della relativa password di accesso.

## 5. Livelli di servizio

### 5.1 Modalità di erogazione

Nel verificare la disponibilità dell'erogazione e, di conseguenza, nel calcolo del livello di servizio, InfoCert considera soltanto le componenti di propria competenza. La figura sottostante (FIG. 2) offre uno schema esemplificativo del dialogo tra l'applicazione del Cliente ed il servizio di conservazione sostitutiva dei documenti LegalDoc Folders, allo scopo di distinguere le parti che rimarranno sotto la responsabilità di InfoCert da quelle di competenza esclusiva del Cliente.

**FIG. 2: Architettura complessiva della soluzione LegalDoc folders**



Per **richiesta** si intenderà l'invocazione delle funzionalità di invio in *conservazione* del documento.

## **5.2 Service Level Agreement (SLA)**

InfoCert, entro 10 giorni lavorativi dall'attivazione del contratto e dalla verifica dei dati indicati dal Cliente nella Richiesta di attivazione, provvede ad assegnare al Cliente un profilo d'abilitazione per l'accesso al Servizio.

Orario di servizio: l'orario di produzione è stabilito come segue:

dal lunedì al venerdì, dalle ore 8:00 alle ore 21:00 ed il sabato dalle ore 8:00 fino alle ore 14:00, esclusi i giorni festivi e le festività infrasettimanali nazionali.

Il Cliente, dal proprio applicativo, potrà richiamare i servizi di LegalDoc Folders, attenendosi alle modalità indicate da InfoCert nello strumento LegalDoc Connector.

Il livello di qualità del servizio di conservazione sostitutiva offerto da InfoCert è garantito dal rispetto dei seguenti requisiti e parametri:

1. InfoCert garantisce, per quanto concerne le componenti *on-line*, una disponibilità del servizio non inferiore al 95 % dell'orario di servizio calcolata sulla base di un mese solare, a partire dal primo giorno di calendario del mese stesso;
2. sono esclusi dal Service Level Agreement tutti i casi di errata configurazione delle apparecchiature del Cliente, tutti i casi di problemi riguardanti le componenti del Cliente o la rete internet e comunque tutti i casi di problemi riguardanti componenti che esulano dalla responsabilità di InfoCert.

### **5.2.1 Criteri di misurazione**

Il Service Level Management (SLM) previsto per questo servizio è regolato da un'unica metrica che si identifica nella “**disponibilità**”.

Il calcolo della disponibilità del servizio viene effettuato facendo riferimento ai minuti di indisponibilità effettivi del servizio nell'orario di produzione concordato, secondo quanto indicato dal presente Allegato Tecnico.

InfoCert verifica il corretto funzionamento dei servizi tramite l'utilizzo di strumenti software, denominate “sonde”, le quali automaticamente e periodicamente simulano una richiesta di servizio da parte del Cliente. Le specifiche di navigazione per queste sonde (es.: quali funzioni richiedere e fino a quale grado di dettaglio scendere) vengono definite da InfoCert, non contemplano attività di aggiornamento, modifica o stampa poiché eseguono automaticamente e frequentemente operazioni che simulano l'attività utente. Qualora il servizio non risponda secondo le modalità concordate, la sonda allerta il sistema di controllo della produzione InfoCert.

L'indisponibilità del **Servizio** sarà dichiarata in uno dei seguenti casi:

- su segnalazione degli strumenti di monitoraggio InfoCert, previo esame e validazione da parte del sistema di controllo della produzione InfoCert, secondo quanto previsto dalle procedure relative al processo “Problem Management” di InfoCert, certificata ISO9001-Vision2000”
- su eventuale segnalazione del disservizio da parte del Cliente, previo esame e validazione da parte del sistema di controllo della produzione InfoCert. Anche in questo caso la segnalazione perviene alla funzione di Problem Manager, il quale registra il disservizio a partire dal momento della segnalazione del Cliente e fino al momento del ripristino del servizio.

### **5.2.2SLA Disponibilità**

InfoCert garantisce una disponibilità effettiva del servizio di LegalDoc Folders non inferiore al 95% (novantacinque per cento), da calcolarsi con periodicità mensile sulla base dell'orario di servizio definito nel paragrafo precedente.

Il parametro di indisponibilità previsto del Servizio A.S.P. è equivalente o minore al 5% della erogazione mensile dello stesso servizio.



## **6. Allegato**

### **6.1 Informazioni sul Data Center**

Nel seguito sono descritte le modalità generali tecniche e le infrastrutture che InfoCert utilizza all'interno del proprio data center di Padova.

#### **Sicurezza fisica**

Lo stabile InfoCert è sorvegliato da personale specializzato 24 ore al giorno; la sala CED, dove si trovano i dispositivi hardware e software dei diversi sistemi d'InfoCert, la sala di controllo dell'alimentazione elettrica, del sistema idraulico, del condizionamento e la sala di monitoraggio dei sistemi di sicurezza installati, è accessibile solo mediante utilizzo di *badge* autorizzato ed è controllato da un sistema TVCC; le porte sono dotate d'allarmi a contatti magnetici; le stanze dell'area sono controllate mediante rivelatori combinati microonde e infrarossi.

Le aree del CED sono dotate d'impianto di rilevazione fumi e antincendio.

#### **Alimentazione elettrica - garanzia gruppi di continuità**

Tutte le apparecchiature del centro dati di Padova di InfoCert sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso d'interruzione dell'erogazione dell'energia elettrica da parte del fornitore. In caso d'assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

#### **Connessione ad Internet attraverso InfoCert**

Il centro dati di InfoCert è connesso alla rete internet con due collegamenti ATM separati entrambi con velocità massima di 155 Mbit/sec. Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati d'interfaccia separati e completamente ridondati. InfoCert è impegnata a mantenere tempi d'attraversamento rete estremamente contenuti (inferiori a 20 ms) tra il proprio Centro Servizi ed i nodi d'interconnessione con i principali Provider italiani ed internazionali.

#### **Sicurezza delle reti: protezione da intrusioni**

I sistemi e le reti di InfoCert sono connessi ad Internet in modo controllato da sistemi *firewall* che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del *firewall*, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "*default deny*" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e "*defense in depth*" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere *firewall*, ed infine a livello di sistema, *hardening*).

La definizione delle politiche d'accesso relativamente ai siti del Cliente sarà concordata, nel rispetto dei vincoli imposti dalle politiche stabilite dall'Area Sistemi di Sicurezza Informatica d'InfoCert.

La gestione e l'implementazione delle regole di sicurezza dei firewall sono stabiliti da InfoCert.

I sistemi firewall InfoCert sono configurati in alta affidabilità (HA), ovvero sono formati da coppie di macchine indipendenti, collegate tra loro e gestite, tramite appositi software, in modo che in caso di guasto di una delle macchine, il traffico venga dirottato sulla macchina di backup.

---

Padova, 22/09/2015

# **CONFIGURAZIONE LEGALDOC AMBIENTE DI PRODUZIONE**

## 1. Dati di configurazione del servizio

Ragione sociale:	Comune di Santa Giustina in Colle
Id bucket:	B33874
Codice account:	J8CDP0
Casella posta certificata:	ragioneria@comunesgcolle.pd.it
Data attivazione:	22/09/2015

## 2. User associate

### 2.1. J8CDP001

Accesso: Abilitato  
Tipo di accesso: WebServices + Interfaccia  
Viewer: Sola lettura  
Impronta: Lettura e creazione

#### Tipologie documentali:

Tipologia documentale	Download	Conserva	Rettifica	Elimina	Ricerca
cad regprot	SI	SI	SI	SI	SI
cstpd atto	SI	SI	SI	SI	SI
cstpd contr	SI	SI	SI	SI	SI
cstpd del	SI	SI	SI	SI	SI
cstpd det	SI	SI	SI	SI	SI

### 3. Policy associate

#### 3.1. P33716 - Policy standard

**Formati di file ammessi alla conservazione:**

File Mime	Descrizione
application/msword;2007	DOCX
application/pkcs7;NA application/msword;2007	DOCX firmato
application/pkcs7;NA application/vnd.ms-excel;2007	XLSX firmato
application/pkcs7;NA application/vnd.ms-outlook;NA	MSG firmato
application/pkcs7;NA application/vnd.ms-powerpoint;2007	PPTX firmato
application/pkcs7;NA application/vnd.oasis.opendocument.graphics;NA	ODG firmato
application/pkcs7;NA application/vnd.oasis.opendocument.presentation;NA	ODP firmato
application/pkcs7;NA application/vnd.oasis.opendocument.spreadsheet;NA	ODS firmato
application/pkcs7;NA application/vnd.oasis.opendocument.text;NA	ODT firmato
application/pkcs7;NA image/gif;NA	GIF firmato
application/pkcs7;NA image/jpeg;NA	JPG firmato
application/pkcs7;NA image/tiff;NA	TIFF firmato
application/pkcs7;NA text/plain;NA	TXT firmato
application/pkcs7;NA text/xml;1.0	XML firmato
application/timestamp-reply;NA application/pkcs7;NA application/msword;2007	DOCX firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.ms-excel;2007	XLSX firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.ms-outlook;NA	MSG firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.ms-powerpoint;2007	PPTX firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.oasis.opendocument.graphics;NA	ODG firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.oasis.opendocument.presentation;NA	ODP firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.oasis.opendocument.spreadsheet;NA	ODS firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA application/vnd.oasis.opendocument.text;NA	ODT firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA image/gif;NA	GIF Firmato e Marcato
application/timestamp-reply;NA application/pkcs7;NA image/jpeg;NA	JPG firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA image/tiff;NA	TIFF firmato e marcato



File Mime	Descrizione
application/timestamp-reply;NA application/pkcs7;NA text/plain;NA	TXT firmato e marcato
application/timestamp-reply;NA application/pkcs7;NA text/xml;1.0	XML firmato e marcato
application/vnd.ms-excel;2007	XLSX
application/vnd.ms-outlook;NA	MSG
application/vnd.ms-powerpoint;2007	PPTX
application/vnd.oasis.opendocument.graphics;NA	ODG
application/vnd.oasis.opendocument.presentation;NA	ODP
application/vnd.oasis.opendocument.spreadsheet;NA	ODS
application/vnd.oasis.opendocument.text;NA	ODT
image/gif;NA	GIF
image/jpeg;NA	JPG
image/tiff;NA	TIFF
text/plain;NA	TXT
text/xml;1.0	XML

**Formati di file indice ammessi:**

File Mime	Descrizione
text/xml;1.0	XML

**Tipologie documentali:**

Nome	Descrizione	Controllo
cad regprot	Registro di protocollo	nessuno
cstpd atto	Atto Amministrativo	nessuno
cstpd contr	Contratto	nessuno
cstpd del	Deliberazione di Giunta o Consiglio	nessuno
cstpd det	Determinazione Dirigenziale	nessuno

**Firmatario:**

Nessun firmatario associato.

## 4. Campi di indice e controlli predefiniti per le Tipologie documentali

### 4.1. REGISTRO DI PROTOCOLLO - cad\_regprot

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	data documento dt	SI	NO	-
Codice identificativo dell'Amministrazione	codice_amm_s	NO	NO	-
Codice identificativo AOO	codice_aoo_s	NO	NO	-
ID univoco	id s	NO	NO	-
Oggetto	oggetto s	SI	NO	-
Numero ine	prot ine i	SI	NO	-
Numero inizio	prot inizio i	SI	NO	-

### 4.2. ATTO AMMINISTRATIVO - cstpd\_atto

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	data documento dt	SI	NO	-
Oggetto	oggetto s	SI	NO	-
Numero Protocollo	protocollo s	SI	NO	-
Numero di Repertorio	repertorio s	SI	NO	-
Tipo Documento	tipo documento s	SI	NO	-
Ufficio Proponente	ufficio s	NO	NO	-

### 4.3. CONTRATTO - cstpd\_contr

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	data documento dt	SI	NO	-
Contraente	contraente s	SI	NO	-
Data Registrazione	data registrazione dt	SI	NO	-
Importo Registrazione	importo registrazione d	SI	NO	-
Numero Registrazione	numero registrazione s	SI	NO	-
Oggetto	oggetto s	SI	NO	-
Numero di Repertorio	repertorio s	SI	NO	-
Serie Registrazione	serie registrazione s	SI	NO	-

**4.4. DELIBERAZIONE DI GIUNTA O CONSIGLIO - cstpd\_del**

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	data documento dt	SI	NO	-
Oggetto	oggetto s	SI	NO	-
Numero di Repertorio	repertorio s	SI	NO	-
Ufficio Proponente	ufficio s	SI	NO	-

**4.5. DETERMINAZIONE DIRIGENZIALE - cstpd\_det**

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	data documento dt	SI	NO	-
Oggetto	oggetto s	SI	NO	-
Numero di Repertorio	repertorio s	SI	NO	-
Ufficio Proponente	ufficio s	NO	NO	-



# ***PROTOCOLLO E ATTI***

## Manuale Operativo

*Documento*

Prodotto .....	s100
Descrizione .....	Protocollo
Revisione del .....	07/01/2013
Versione.....	10.04.00
Autore .....	Kibernetes s.r.l. – Team Segreteria
Formato file .....	MSWord2000
Nome file.....	:

Le informazioni contenute nella presente documentazione sono soggette a modifiche senza preavviso.

Se non specificato diversamente, ogni riferimento a società, nomi, dati e indirizzi utilizzati negli esempi è puramente casuale ed ha il solo scopo di illustrare il contenuto della documentazione.

Le istruzioni e descrizioni di questo manuale sono accurate relativamente al momento di stampa .

Il prodotto documentato e la stessa documentazione possono successivamente essere oggetto di cambiamenti senza preavviso.

Kibernetes Srl non si assume responsabilità per possibili danni diretti o indiretti causati da errori, omissioni o discrepanze tra il prodotto documentato e questa documentazione.

**TUTTI I DIRITTI SONO RISERVATI.** Senza il **PERMESSO SCRITTO DI KIBERNETES** Srl nessuna parte del manuale può essere riprodotta, archiviata in un sistema che permetta la riproduzione, o trasmessa in ogni forma, sia elettronica, meccanica, in fotocopia, registrata o altre.

Copyright © by Kibernetes s.r.l. - Silea (Italia) -  
All rights reserved.

## Indice

<b>1</b>	<b>INTRODUZIONE .....</b>	<b>5</b>
	Scopo del manuale .....	5
	Specifiche tecniche .....	5
<b>2</b>	<b>PROTOCOLLO .....</b>	<b>6</b>
<b>2.1</b>	<b>APERTURA DEL PROGRAMMA.....</b>	6
<b>2.2</b>	<b>INSERIMENTO CAMPI OBBLIGATORI.....</b>	7
<b>2.3</b>	<b>NUOVO SOGGETTO.....</b>	10
<b>2.4</b>	<b>GESTIONE MITTENTE.....</b>	15
<b>2.5</b>	<b>DESTINATARI INTERNI.....</b>	17
<b>2.6</b>	<b>ARCHIVIAZIONE.....</b>	21
<b>2.7</b>	<b>CREAZIONE SCHEMA.....</b>	23
<b>2.8</b>	<b>NOTE, NOTE RISERVATE, PERIODO DI PUBBLICAZIONE, FASCIOLI E</b>	
	<b>RELAZIONI.....</b>	24
<b>2.9</b>	<b>RISERVATEZZA.....</b>	28
<b>2.10</b>	<b>ANNULLAMENTO PROTOCOLLO.....</b>	31
<b>2.11</b>	<b>STAMPA RICEVUTA .....</b>	32
<b>2.12</b>	<b>INVIA TRAMITE MAIL.....</b>	33
<b>2.13</b>	<b>CREA SUSSEGUENTE.....</b>	35
<b>3</b>	<b>FUNZIONE CERCA .....</b>	<b>36</b>
<b>4</b>	<b>REGISTRO D'EMERGENZA.....</b>	<b>40</b>
<b>5</b>	<b>STAMPA DEI REGISTRI.....</b>	<b>42</b>
<b>6</b>	<b>FUNZIONALITÀ E UTENTI .....</b>	<b>51</b>
<b>7</b>	<b>FUNZIONE DI NAVIGAZIONE "VAI A .." .....</b>	<b>53</b>



## INDICE DELLE FIGURE

<b>Figura 1</b> - Apertura Applicativo .....	6
<b>Figura 2</b> – Nuovo Protocollo .....	7
<b>Figura 3</b> - Inserimento Dati.....	8
<b>Figura 4</b> - Nuovo Soggetto .....	10
<b>Figura 5</b> - Nuovo Soggetto .....	11
<b>Figura 6</b> - Assegna Soggetto.....	12
<b>Figura 7</b> - Aggiungi mittenti.....	12
<b>Figura 8</b> - Aggiungi mittenti.....	16
<b>Figura 9</b> - Aggiungi mittenti.....	16
<b>Figura 10</b> - Aggiungi mittente .....	17
<b>Figura 11</b> - Destinatari interni.....	18
<b>Figura 12</b> – Gestione destinatari.....	19
<b>Figura 13</b> – Gestione destinatari.....	20
<b>Figura 14</b> – Titolare d’archivio .....	21
<b>Figura 15</b> – Titolare d’archivio .....	22
<b>Figura 16</b> – Schema protocollo.....	23
<b>Figura 17</b> - Gestione Note.....	24
<b>Figura 18</b> - Numero Protocollo.....	26
<b>Figura 19</b> - Modifica Protocollo .....	28
<b>Figura 20</b> - Modifica Protocollo .....	29
<b>Figura 21</b> – Rendi riservato .....	30
<b>Figura 22</b> - Togli riservatezza.....	30
<b>Figura 23</b> - Annullamento Protocollo .....	31
<b>Figura 24</b> - Annullamento Protocollo .....	31
<b>Figura 25</b> – Stampa ricevuta .....	32
<b>Figura 26</b> - Crea susseguente.....	32
<b>Figura 27</b> - Ricerca Testuale.....	37
<b>Figura 28</b> - Ricerca Testuale.....	37
<b>Figura 29</b> - Ricerca Puntuale .....	39
<b>Figura 30</b> – Registro di emergenza .....	41
<b>Figura 31</b> - Stampa Registro .....	42
<b>Figura 32</b> - Stampa Registro .....	43
<b>Figura 33</b> - Stampa Registro .....	44
<b>Figura 34</b> - Stampa Registro .....	45
<b>Figura 35</b> - Stampa Registro .....	46
<b>Figura 36</b> - Stampa Registro .....	47
<b>Figura 37</b> - Stampa Registro .....	48
<b>Figura 38</b> - Stampa Registro .....	50
<b>Figura 39</b> - Utente Generico .....	51
<b>Figura 40</b> - Utente Generico .....	52
<b>Figura 41</b> - Utente Generico .....	52
<b>Figura 42</b> – Funzione di navigazione.....	53
<b>Figura 43</b> – Elenco delle operazioni eseguite .....	54

## 1 INTRODUZIONE

### Scopo del manuale

Lo scopo di questo manuale è di fornire all'utente, che si appresta ad utilizzare questa nuova procedura, le informazioni necessarie per essere il più possibile autonomo nelle operazioni principali di gestione del Protocollo Informatico.

Esso rappresenta una guida veloce e facilmente consultabile per poter svolgere le attività più importanti nelle fasi di registrazione, consultazione e archiviazione del protocollo.

### Specifiche tecniche

L'applicativo Protocolli e Atti è uno strumento software che utilizza le migliori tecnologie attualmente disponibili nel mondo informatico. Utilizza la tecnologia **LOTUS** per il lavoro di gruppo, e **Crystal Report** per la produzione di stampe ed è sviluppato in ambiente **Java**. È nativo **ASP** ed è portabile su tutte le più diffuse piattaforme operative (**Windows, Linux, Oracle**). È dotato di funzioni che rispondono totalmente ai requisiti contenuti nel D.P.R. 445 del 28/12/2000 e a tutte le linee guida del Dipartimento dell'Innovazione Tecnologica.

L'interfaccia di comunicazione tra operatore e sistema, è sviluppata secondo standard che ne consentono una visualizzazione mediante il browser Internet Explorer. La navigazione all'interno del programma, pertanto si apprende facilmente ed è di facile utilizzo. Ogni campo all'interno del quale l'operatore introduce le informazioni richieste, ha una intestazione che solitamente si trova in alto a destra del Campo stesso che aiuta a comprendere le informazioni da inserire.

Oltre alla descrizione dettagliata delle principali funzionalità implementate, la presente guida dispone di un ricco repertorio di immagini che semplificano ulteriormente la comprensione dell'applicativo. Su ogni immagine sono state inserite delle caselle di testo riassuntive e altri simboli che possano aiutare a comprendere in maniera puntuale ogni singola fase del processo di registrazione del protocollo e le successive fasi di analisi e ricerca.

## 2 PROTOCOLLO

### 2.1 Apertura del Programma

Figura 1 - Apertura Applicativo

L'interfaccia del programma Protocolli e Atti come si può notare dalla, è simile ad una pagina Web e, rispetto ad essa, segue le stesse logiche di funzionamento.

La prima operazione che si rende necessaria per attivare l'applicativo è di specificare l'indirizzo del server operazione che, viene effettuata senza l'intervento dell'operatore.

Per rendere operativa la fase di registrazione del protocollo occorre cliccare sul bottone **"Nuovo Protocollo"**

La funzione **Cerca Protocollo** consente di ricercare rapidamente un protocollo inserendo prima l'anno e poi il numero di protocollo.

Funzione di navigazione: per l'utilizzo della funzione vedere il paragrafo **"Funzione Vai a ..."**

Questa area contiene le informazioni di sintesi del protocollo ed in particolare: l'**Anno di riferimento**, la **Data**, l'**Oggetto**, l'**Unità Organizzativa** e gli **Intestatori**. Al momento, tale videata, risulta vuota perché non è stata registrata nessuna informazione.

Fi

## 2.2 Inserimento Campi Obbligatori

Effettuate le operazioni preliminari necessarie per l'apertura del programma, l'applicativo è pronto. Alcune delle voci che sono visualizzate sulla parte superiore dell'interfaccia in Figura 2 (per anno, per unità organizzativa, per fascicolo, ricevuti, rifiutati) verranno commentate successivamente quando il database è alimentato da un numero sufficiente di informazioni.

La registrazione di un nuovo protocollo si attiva cliccando sul pulsante "Nuovo Protocollo" come evidenziato nella Figura 2. Nell'applicativo viene visualizzata una maschera composta da una serie di campi che l'operatore è tenuto a completare.

I campi contrassegnati con un asterisco sono gli unici obbligatori secondo le disposizioni previste dal D.P.R. 445/2000. Tuttavia è bene abituarsi a completare tutte le altre voci di cui si dispongono le informazioni al fine di consentire, in una fase successiva, di rintracciare le informazioni relative al protocollo in maniera veloce ed efficace.

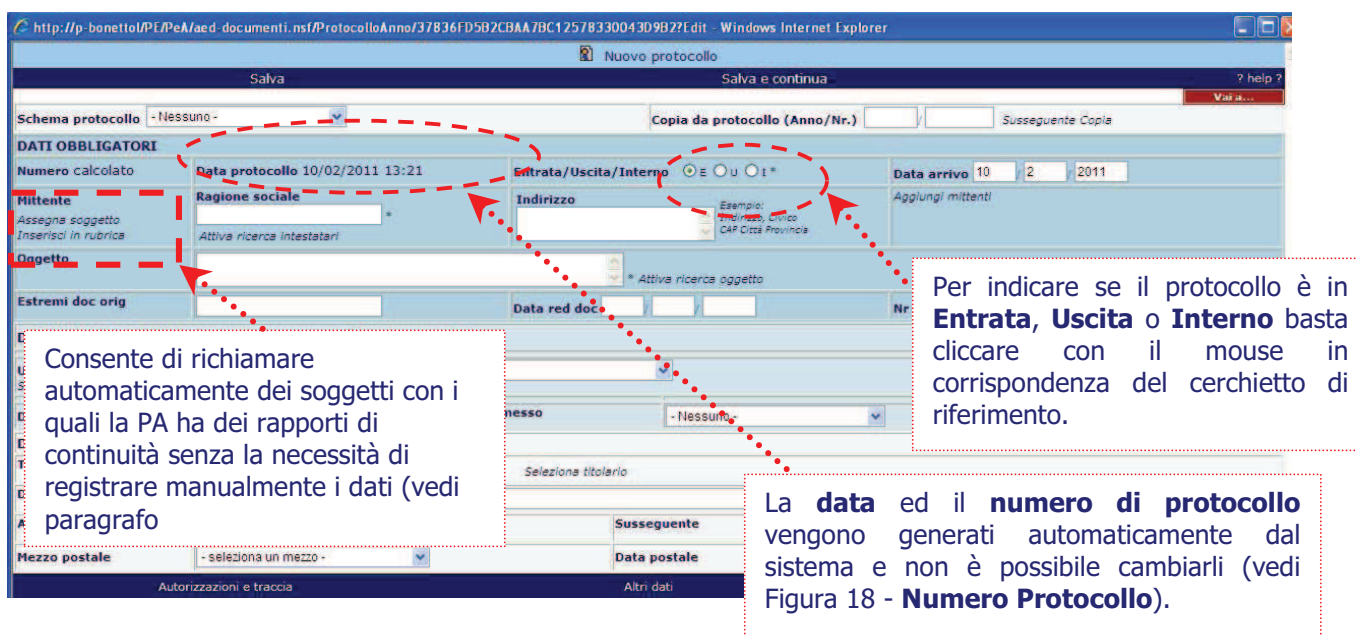


Figura 3 - Inserimento Dati

La data ed il numero di protocollo vengono generati automaticamente dal sistema non appena le informazioni obbligatorie sono state salvate. Questa funzionalità è stata introdotta per cautelare l'operatore nel caso in cui attiva il protocollo senza la necessità di registrare delle informazioni e quindi di produrre dei protocolli vuoti. È utile ricordare che una volta che il protocollo è stato creato (e quindi esiste un Numero Protocollo) non è più possibile eliminarlo fisicamente dal sistema ma è possibile solamente Annullarlo, operazione che descriveremo nel seguito del manuale (vedi pagina 31).

Il Numero Protocollo, come previsto dalla normativa vigente, è composto da due parti: la prima rappresenta l'anno di riferimento, la seconda è un numero progressivo. Ad esempio, il primo protocollo dell'anno 2006 sarà "2006 1", il secondo "2006 2", l'*n*-esimo protocollo "2006 *n*". Una volta che il sistema assegna il numero di protocollo, non è possibile in alcun modo modificarlo.

Altro campo obbligatorio è quello che riguarda il protocollo in Entrata, in Uscita o Interno. Il sistema indica di default, cioè automaticamente, l'opzione "Entrata", questo perché tipicamente il protocollo in entrata è quello maggiormente utilizzato nelle amministrazioni. Tuttavia, per selezionare le altre opzioni è sufficiente cliccare con il mouse in corrispondenza del cerchietto di riferimento (Vedi Figura 3). È consigliabile verificare sempre, soprattutto nelle prime registrazioni che l'opzione selezionata dal sistema sia quella corretta.

I campi successivi sono relativi all'intestatario. Nella compilazione del protocollo è obbligatorio indicare il soggetto che ha attivato il procedimento amministrativo. L'applicativo gestisce questa informazione attraverso il campo "Ragione Sociale" all'interno del quale il protocollista è tenuto ad indicare i riferimenti anagrafici del soggetto. È possibile inserire anche

l'indirizzo che non è un campo obbligatorio ma, per le considerazioni sopra esposte, rappresenta una informazione che può risultare particolarmente interessante in fase successiva di ricerca.

È possibile caricare i dati del mittente/destinatario utilizzando quanti già presenti in archivio protocollo.

La funzione si attiva cliccando sulla funzione "Attiva ricerca intestatari".

<b>Mittente</b> <i>Assegna soggetto</i> <i>Inserisci in rubrica</i>	<b>Ragione sociale</b> <input type="text"/> * <a href="#">Attiva ricerca intestatari</a>
---	--

Attivata la ricerca, apparirà **LiveSearch attivato** ad indicare che la ricerca è attiva.

<b>Mittente</b> <i>Assegna soggetto</i> <i>Inserisci in rubrica</i>	<b>Ragione sociale</b> <input type="text"/> * <b>LiveSearch attivato</b> <a href="#">Disattiva ricerca intestatari</a>
---	---

La ricerca produrrà effetti digitando almeno 3 caratteri

<b>Mittente</b> <i>Assegna soggetto</i> <i>Inserisci in rubrica</i>	<b>Ragione sociale</b> <input type="text" value="ross"/> * Rossi Marco rossi marco - Via Indipendenza 330020 Musile di Piave VE rossi marco - Via Indipendenza, 330020 Musile di Piave - VE rossi mario - sede	<b>Indirizzo</b> <input type="text"/>
<b>Oggetto</b>		

I dati verranno presentati una sola volta per ogni ricorrenza trovata comprensiva dei dati di indirizzo (se un soggetto è associato a diversi indirizzi, verrà presentati con tutti gli indirizzi trovati). Con il cursore sarà quindi possibile scegliere il dato desiderato.

Per favorire una più rapida compilazione del protocollo e una maggiore uniformità negli oggetti ( e quindi maggiore affidabilità nelle ricerche ), esiste una funzione che consente di digitare alcune lettere dell'oggetto di protocollo ed ottenere in elenco tutti gli oggetti che iniziano con tali lettere.

La funzione, attivabile su richiesta dell'operatore laddove si desidera un supporto alla scrittura, si chiama "Attiva ricerca oggetto" ed è presentata a destra del campo oggetto del protocollo.

<b>Oggetto</b>	<input type="text"/> * <a href="#">Attiva ricerca oggetto</a>
----------------	---

Attivata la funzione, appare l'informazione **LiveSearch attivato**. Per ottenere l'avvio della ricerca è necessario digitare almeno 5 caratteri ( con meno di 5 caratteri la funzione non produce effetti ).

Il risultato presentato è del tipo in figura



<b>Oggetto</b>	richiesta pub	* LiveSearch attivato
<b>RIFERIMENTI INTERNI</b>	Richiesta pubblicazione all'albo	
<b>Documento collegato</b>	richiesta pubblicazione all'albo bando di concorso	
<b>UO</b>	richiesta pubblicazione all'albo del comune di loro bando di gara	
<i>Seleziona UO</i>	Richiesta pubblicazione informativa su bando di concorso. maggiori informazioni sul sito internet del comune di pescantina	
<b>Responsabile</b>		

Con il mouse o spostandosi con le frecce si seleziona il risultato desiderato

Se si digita una parte dell'oggetto e successivamente si clicca su "Attiva LiveSearch" per ottenere i corrispondenti oggetti è necessario aggiungere o togliere almeno un carattere a quanto già digitato ( ricordiamo comunque la necessità che vi siano almeno 5 caratteri digitati ).

## 2.3 Nuovo Soggetto

Alcuni soggetti hanno rapporti di continuità con l'Amministrazione ad esempio i gestori telefonici, l'ENEL ecc... Per questo motivo, e per semplificare ulteriormente la registrazione, è possibile inserire i dati anagrafici relativi a questi soggetti in un apposito archivio generato dall'applicativo e renderli disponibili all'operatore nel momento della registrazione. Per attivare questa funzione è sufficiente cliccare con il mouse su "Assegna Soggetti" (vedi). L'applicativo, in questo caso, visualizza i soggetti precedentemente registrati nell'archivio come evidenziato nella Figura 6. Una ulteriore pressione del mouse in corrispondenza del soggetto consente di registrare i dati nei campi relativi. Per registrare invece un "Nuovo soggetto",che ancora non fa parte dell'archivio, occorre selezionare nella sezione Anagrafiche la voce "Soggetti" Figura 4.



Figura 4 - Nuovo Soggetto Per registrare un nuovo soggetto occorre selezionare **Soggetti** nella sezione Anagrafiche e successivamente **Nuovo Soggetto**.

A questo punto l'applicativo apre una finestra (vedi Figura 5) nella quale occorre riempire i campi con i dati relativi al nuovo soggetto e successivamente cliccare sul bottone "Salva" per rendere effettiva la registrazione del Soggetto. A partire da questo momento e per tutte le operazioni future, il Soggetto registrato sarà presente in archivio.

**Nuovo soggetto** ? help ?

**Salva** Vai a...

<b>Persona/Società P/S</b>		<input type="radio"/> Persona <input type="radio"/> Società*
<b>Nome</b>	<input type="text"/>	*
<b>Cognome</b>	<input type="text"/>	*
<b>Detto</b>	<input type="text"/>	
		<input type="radio"/> Maschio <input type="radio"/> Femmina
	<input type="text"/>	
	<input type="text"/>	
	Nr. <input type="text"/> / <input type="text"/> Scala <input type="text"/> Int. <input type="text"/>	
<b>C.a.p.</b>	<input type="text"/>	
<b>Città</b>	<input type="text"/>	
<b>Prov.</b>	- seleziona una provincia -	
<b>Telefono</b>	<input type="text"/>	
<b>E-mail</b>	<input type="text"/>	
<b>Numero del cellulare</b>	<input type="text"/>	
<b>Accorpamento</b>	<input type="text"/>	
<b>Dati di nascita</b>		
<b>Data di nascita</b>	<input type="text"/> / <input type="text"/> / <input type="text"/>	
<b>Comune di nascita</b>	<input type="text"/>	

Una volta che i dati anagrafici sono stati inseriti occorre salvarli, dopodiché saranno disponibili per tutti gli inserimenti futuri.

**Figura 5** - Nuovo Soggetto

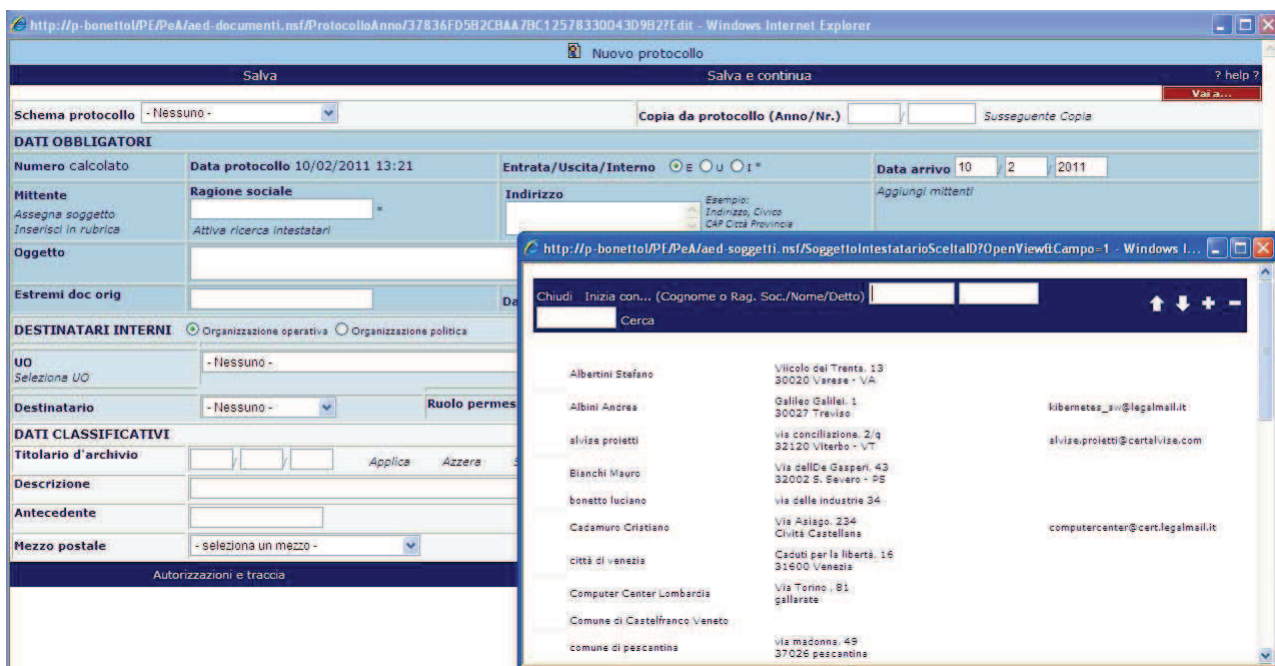


Figura 6 - Assegna Soggetto

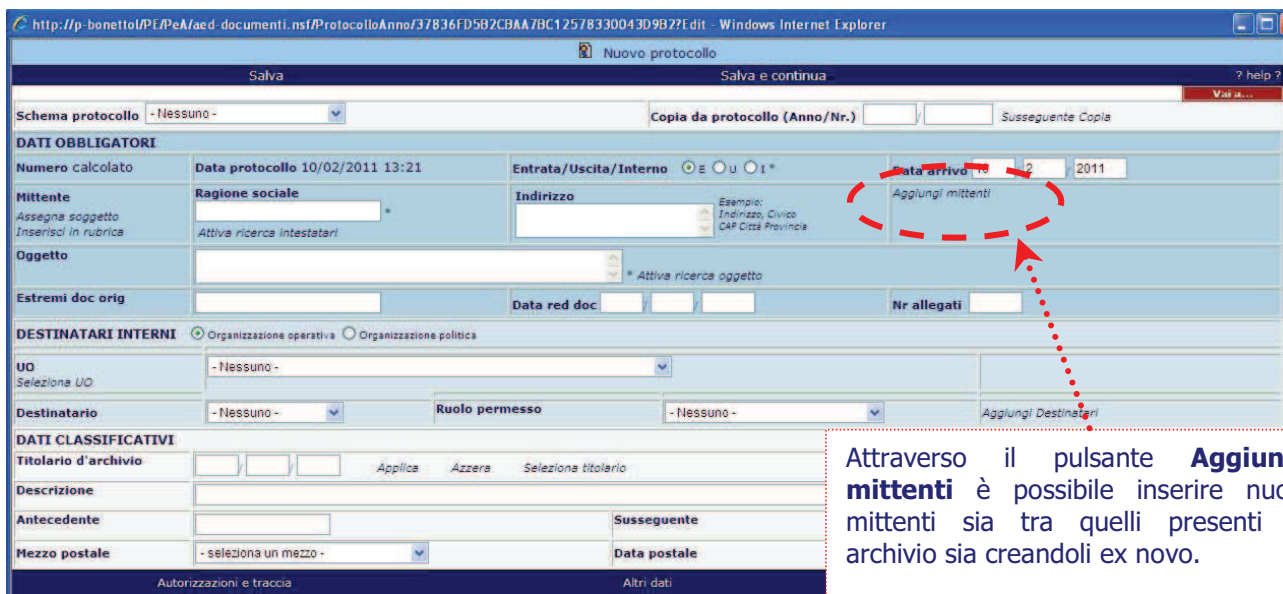


Figura 7 - Aggiungi mittenti

Esiste una funzione che consente di caricare in modo più rapido nuovi mittenti / destinatari nell'archivio dei soggetti.

La maschera di caricamento si presenta con questa informazione

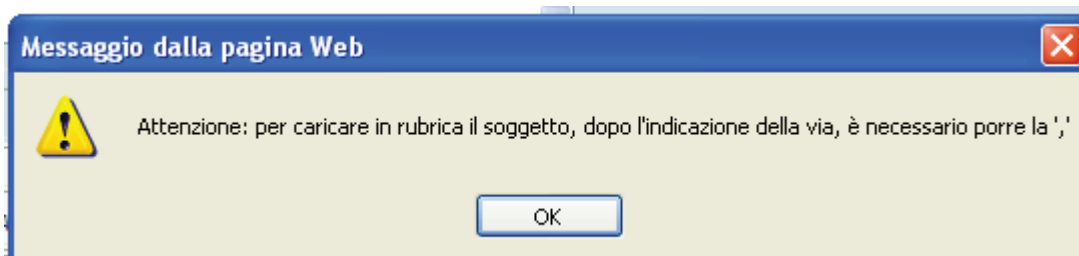


L'operatore che intende inserire automaticamente un nuovo riferimento di posta è invitato a scrivere l'indirizzo seguendo le regole di compilazione descritte ovvero

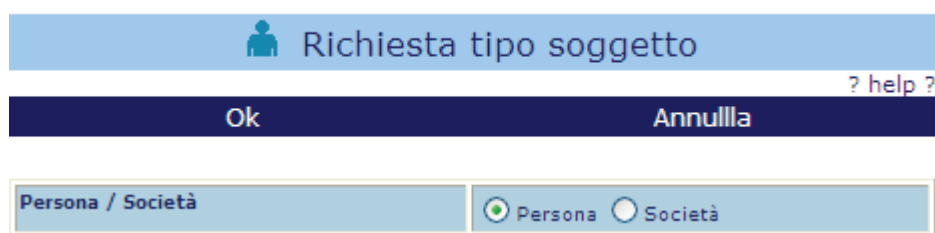
"indirizzo", <spazio> "numero civico"/"Scala (se presente)"<spazio>"Interno (se presente)"  
"C.A.P."<spazio> "Città"<spazio>"sigla della provincia"

Completata la digitazione dei dati, cliccando sulla funzione "Inserisci in rubrica"

l'applicativo, se la struttura dei dati non è stata rispettata ( ovvero non è stata inserita la "virgola" dopo l'indirizzo ), inviterà l'operatore a correggere i dati inseriti



Se i dati sono stati correttamente inseriti, chiederà all'operatore se si tratta di persona fisica o società



Cliccando quindi su "Ok", all'operatore verranno, con oggi, segnalati eventuali soggetti simili a quello appena digitato per evitare di inserire più volte uno stesso soggetto i momenti diversi. Se questi vorrà procedere con l'inserimento del dato, potrà cliccare su "nuovo soggetto" e procedere comunque all'inserimento del dato.



■	Bianchi Mauro	Via dell'De Gasperi, 43 32002 S. Severo - PS
---	---------------	---

Se la ricerca non produce alcun risultato, la funzione di caricamento del nuovo soggetto sarà automatica e produrrà la compilazione di tutte le informazioni digitate nella scheda dei nuovi soggetti.

La scheda verrà presentata all'operatore per consentirgli, se lo ritiene utile, di inserire anche i dati di telefono ed e-mail. Cliccando "salva" completa l'operazione.

Il campo oggetto è l'ultimo dei campi obbligatori per la registrazione del protocollo.

Per favorire una più rapida compilazione del protocollo e una maggiore uniformità negli oggetti ( e quindi maggiore affidabilità nelle ricerche ), una funzione consente di digitare alcune lettere dell'oggetto di protocollo ed ottenere in elenco tutti gli oggetti che iniziano con tali lettere.

La funzione, attivabile su richiesta dell'operatore laddove si desidera un supporto alla scrittura, si chiama "Attiva ricerca oggetto" ed è presentata a destra del campo oggetto del protocollo.

Attivata la funzione, appare l'informazione **LiveSearch attivato**. Per ottenere l'avvio della ricerca è necessario digitare almeno 5 caratteri ( con meno di 5 caratteri la funzione non produce effetti ).

Il risultato presentato è del tipo in figura

<b>Oggetto</b>	richiesta pub	* LiveSearch attivato
<b>RIFERIMENTI INTERNI</b>	Richiesta pubblicazione all'albo	
<b>Documento collegato</b>	richiesta pubblicazione all'albo bando di concorso	
<b>UO</b> <i>Seleziona UO</i>	richiesta pubblicazione all'albo del comune di loro bando di gara	▼
<b>Responsabile</b>	Richiesta pubblicazione informativa su bando di concorso. maggiori informazioni sul sito internet del comune di pescantina	

Con il mouse o spostandosi con le frecce si seleziona il risultato desiderato

Se si digita una parte dell'oggetto e successivamente si clicca su "Attiva LiveSearch" per ottenere i corrispondenti oggetti è necessario aggiungere o togliere almeno un carattere a quanto già digitato ( ricordiamo comunque la necessità che vi siano almeno 5 caratteri digitati ).

Fin tanto che i campi obbligatori non vengono registrati, non è possibile procedere al salvataggio dei dati né tanto meno, generare il numero di protocollo.

Il campo sottostante a quello relativo all'Oggetto, riguarda gli Estremi del Documento Originale, è un campo non obbligatorio all'interno del quale è possibile inserire informazioni utili che si riferiscono al documento che si sta per protocollare.

## 2.4 Gestione Mittente

Nel seguito descriveremo brevemente le informazioni che completano la fase di registrazione del documento e che, pur non obbligatorie per legge, si rendono utili in una fase successiva di ricerca e comunque obbediscono al principio della trasparenza ed efficienza amministrativa.

Abbiamo visto come sia possibile indicare l'intestatario sia digitando manualmente i dati sia ricorrendo all'archivio precedentemente predisposto nel caso si tratti di un soggetto con il quale l'amministrazione ha frequenti rapporti di comunicazione. Tuttavia, è possibile inserire più di un mittente all'interno di uno stesso protocollo, ricorrendo al pulsante "Aggiungi mittenti".



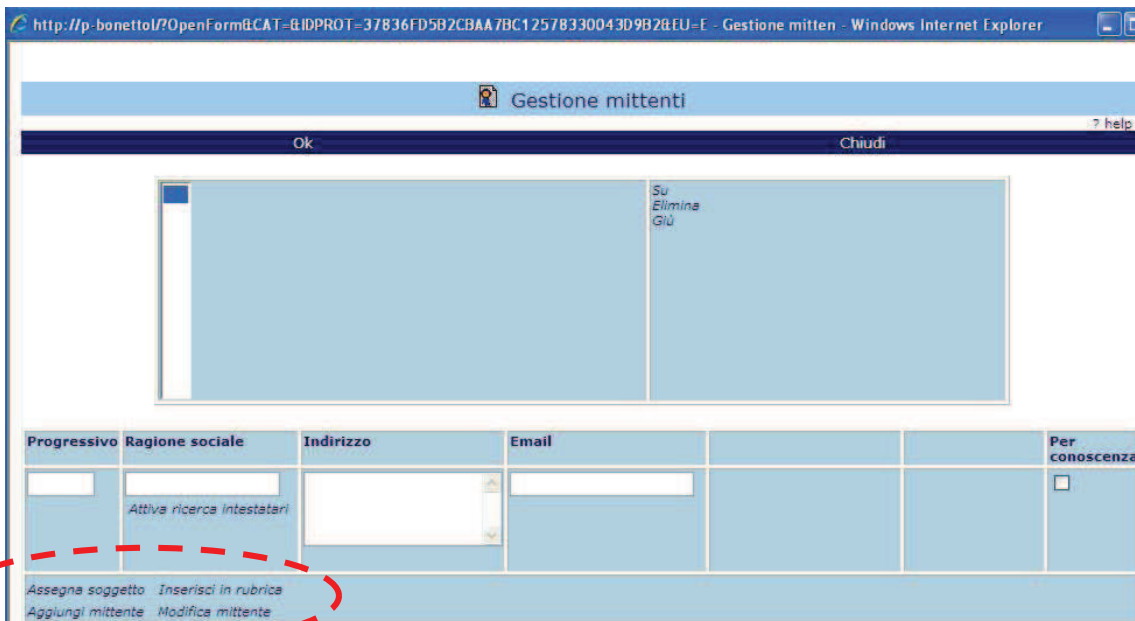


Figura 8 - Aggiungi mittenti

La sezione che in Figura 8 risulta tratteggiata, consente di gestire le informazioni relative ai mittenti.

Il pulsante “Assegna Soggetto” attiva la maschera visualizzata in Figura 9.

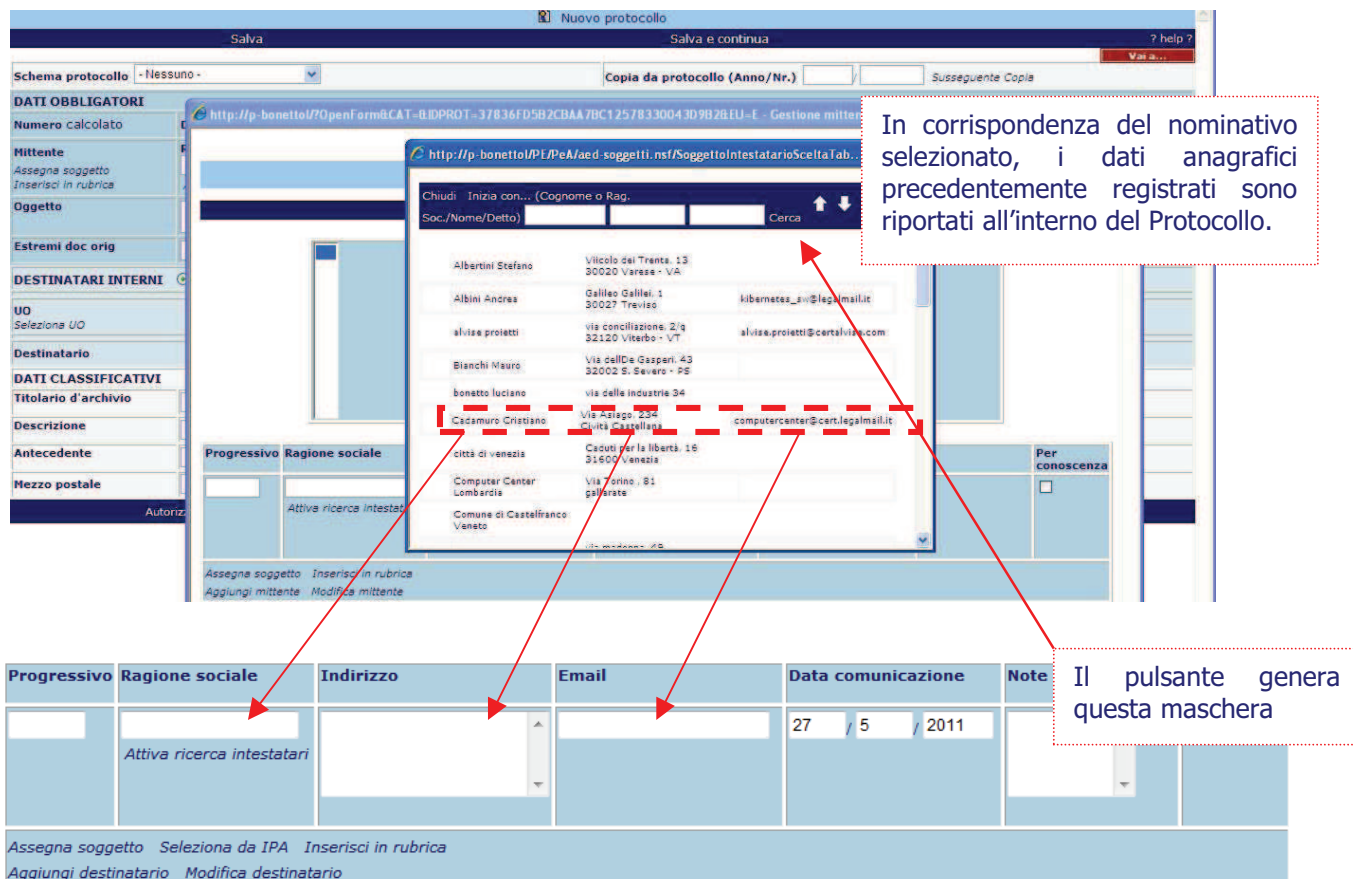


Figura 9 - Aggiungi mittenti

Una volta verificati i dati anagrafici, occorre cliccare sul pulsante “Aggiungi mittenti”. Nel caso in cui i dati inseriti non corrispondano a quelli desiderati oppure si vuole procedere ad annullare l’operazione, occorre cliccare su “Modifica mittente”.

Nel caso in cui i mittenti del protocollo non siano registrati nella sezione “Soggetti”, occorre inserire manualmente i dati all’interno dei campi “Ragione Sociale” e “Indirizzo” Figura 9 e successivamente cliccare sul pulsante “Aggiungi mittente”.

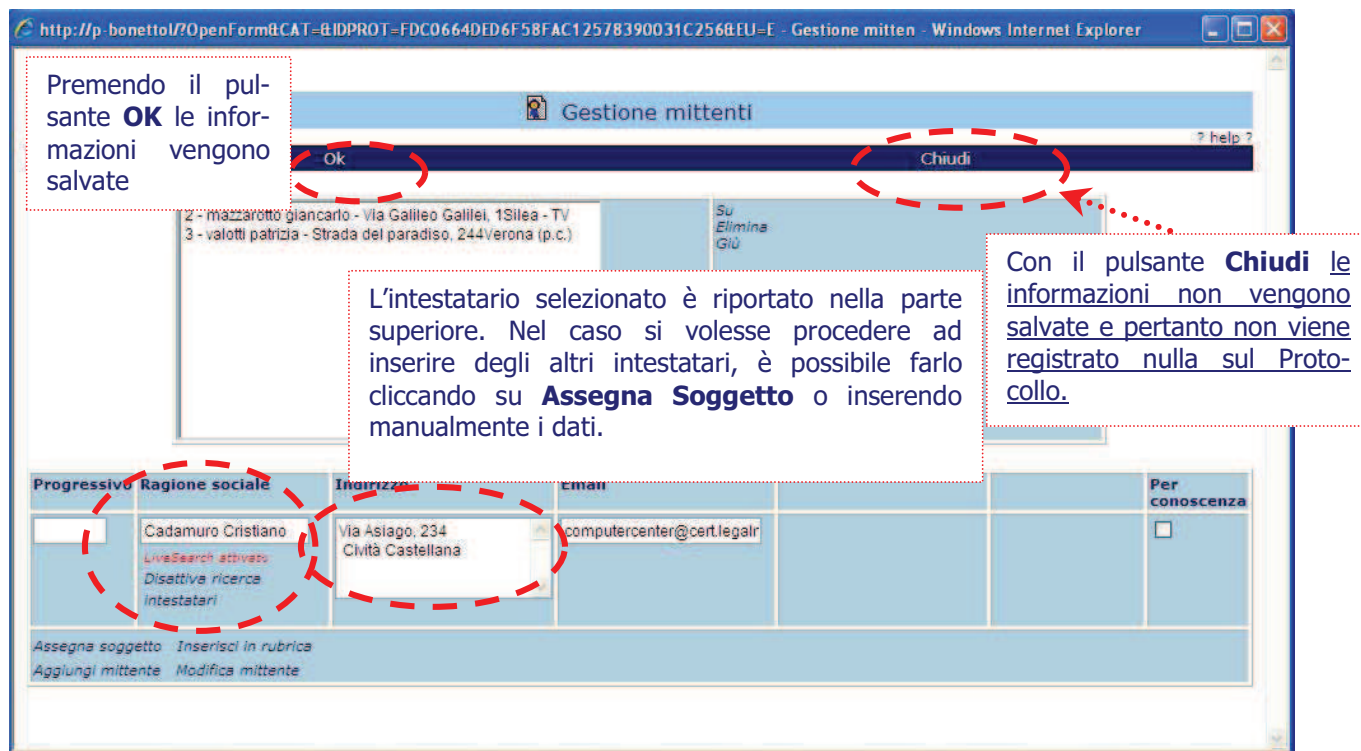


Figura 10 - Aggiungi mittente

L’applicativo è molto flessibile e consente di eliminare un mittente anche quando questo è registrato. Per fare questo occorre selezionare il suddetto e premere sul pulsante Elimina. Gli altri due pulsanti “Su” e “Giù” permettono di cambiare l’ordine di apparizione sullo schermo degli intestatari.

## 2.5 Destinatari Interni

Ogni documento in entrata, dopo essere stato protocollato, viene inviato ad un responsabile o ad un ufficio di competenza. Questa funzionalità viene attivata attraverso la sezione Destinatari

Interni (Figura 11) la metodologia utilizzata è simile a quella impiegata per assegnare un Nuovo Soggetto.



I destinatari del documento sono delle risorse interne all'amministrazione precedentemente inserite in un apposito database. Nel momento in cui si clicca sul pulsante "Aggiungi Destinatari" una schermata relativa alla "Gestione Destinatari", consente di recuperare in maniera molto veloce le informazioni relative ai destinatari del documento senza dover digitare manualmente i dati.

I passaggi che occorre effettuare per assegnare più destinatari, sono i seguenti:

1. Si clicca sul pulsante "Aggiungi Destinatari" (vedi Figura 11);
2. Viene visualizzata la schermata "Gestione Destinatari" sulla quale si seleziona il funzionario (vedi Figura 12);
3. Si clicca su "Aggiungi destinatario" per confermare la scelta (vedi Figura 13)
4. Dopo aver effettuato le operazioni precedenti, l'utente può scegliere di salvare le informazioni inserite cliccando sul pulsante "OK" oppure può decidere di non salvare le informazioni ed in questo caso clicca sul pulsante "Chiudi" (vedi Figura 13).

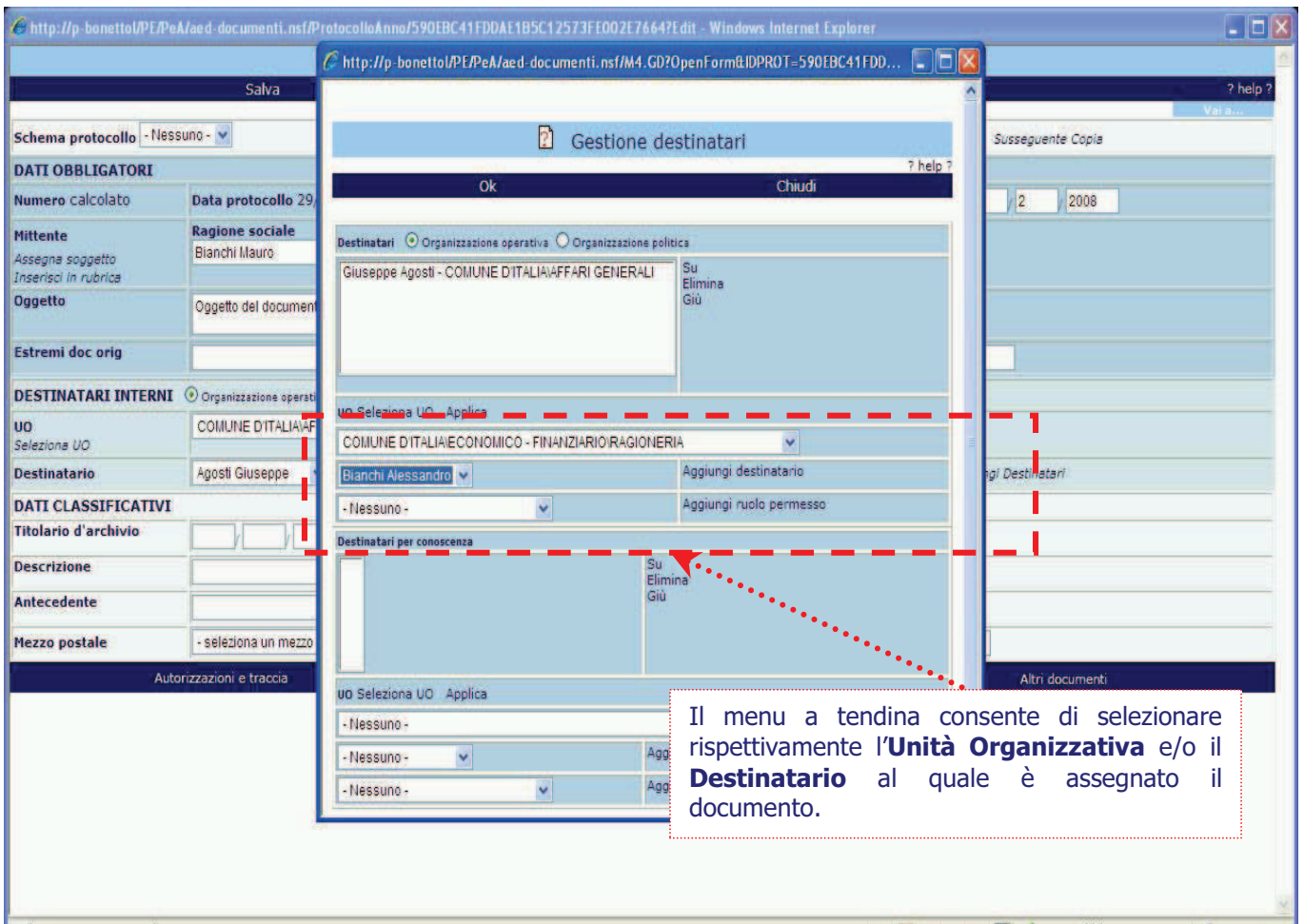
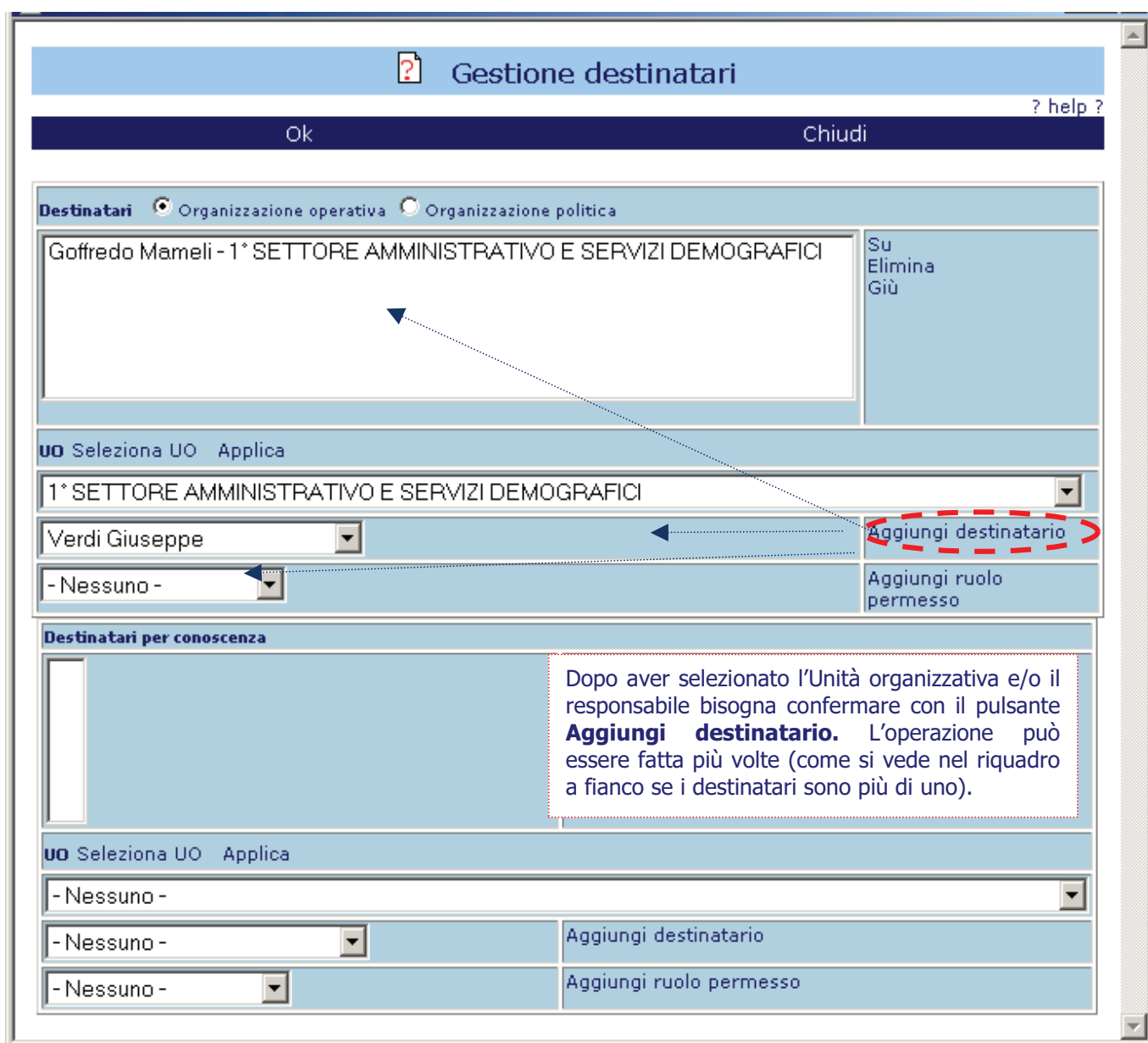


Figura 12 – Gestione destinatari



**Figura 13** – Gestione destinatari

Se un nominativo, ad esempio “Goffredo Mameli” nell’esempio del riquadro in Figura 13, non fa parte dei destinatari, è possibile selezionarlo e successivamente eliminarlo ricorrendo al pulsante Elimina.

Tutta questa procedura è vanificata se dopo aver effettuato le operazioni descritte si preme il pulsante “Chiudi”, per salvare correttamente bisogna invece cliccare sul pulsante **OK**.

## 2.6 Archiviazione

Ogni documento è correttamente archiviato, quando ad esso è assegnato:

- ❖ Titolo
- ❖ Classe
- ❖ Sottoclasse (nel titolario della Soprintendenza per i Beni Archivistici la sottoclasse è facoltativa)



Figura 14 – Titolario d'archivio

Mentre i Titoli sono assegnati per legge e non sono modificabili, le Classi e le Sottoclassi sono creati sulla base delle esigenze della singola amministrazione. Per creare una nuova classe o sottoclasse è sufficiente cliccare sul pulsante Titolario d'archivio dal menu Anagrafiche (vedi Figura 14), riempire i campi (Figura 15) e premere su Salva (si trova in alto a sinistra).



Titolario d'archivio

Salva Salva e continua ? help ?

Vai a...

Categoria	1 Categoria 1 ▾ *
Classe	2 classe 2 ▾
Sottoclasse	- Nessuno - ▾
Nuova sottoclasse	<input type="text"/>
Data di inizio validità	11
Data di fine validità	<input type="text"/>

Il Titolario d'archivio gestisce le informazioni relative alla creazione di una nuova **classe** o **sottoclasse**.

Figura 15 – Titolario d'archivio

Contestualmente all'inserimento di una nuova **classe** o **sottoclasse** si può specificare una **data di inizio** e una di **fine validità** in modo da inibire tale classificazione automaticamente.

## 2.7 Creazione Schema

L'archiviazione di determinati protocolli, richiede l'assegnazione di un Titolo, Classe e Sottoclasse. Per questo motivo, l'applicativo consente di creare degli schemi predefiniti che completano automaticamente le informazioni richieste. Per creare un nuovo schema occorre selezionare il pulsante Schema che si trova nella sezione relativa ai PROTOCOLLO posizionata sulla parte sinistra dell'interfaccia (vedi Figura 16 – **Schema protocollo**).

Dopo aver completato le informazioni richieste in particolare, identificativo e descrizione, si può procedere ad assegnare un titolo, una classe ed eventualmente una sottoclasse che saranno attribuite sempre allo schema prescelto. Per cambiare le impostazioni attribuite ad un determinato schema occorre selezionarlo e successivamente premere sul pulsante Modifica.

Utente:  
Marco Perillo  
Cambia password  
Esci

Scrivania Virtuale

In evidenza:  
Documenti  
Pareri da evadere  
Proposte rifiutate  
Fasi eff. da evadere  
Atti ric. in bozza  
Ricerca estesa

ANAGRAFICHE  
DOCUM.  
APPUN.  
FASCIO  
PROCEE  
PROTO.  
PROPO.  
ALBO P.  
CONTR.  
STATIS.  
STAMPE  
SCHEMI  
Documenti  
Fascicoli  
Protocolli  
Atti  
Contratti  
PROGRESSIVI  
AMMINISTRAZIONE  
Informazioni  
Installazione client

SCHEMA PROTOCOLLO: schema invito 1

Salva Elimina

Identificativo schema	schema invito 1 *															
Descrizione	schema invito 1 *															
Entrata / Uscita / Interno	<input type="radio"/> E <input checked="" type="radio"/> U <input type="radio"/> I															
Oggetto	Invito a partecipazione del sindaco alla serata di beneficenza associa															
Destinatari esterni	<table border="1"> <thead> <tr> <th>Destinatari</th> <th>Email</th> <th>Tipo invio</th> </tr> </thead> <tbody> <tr> <td>1 - Bianchi Mauro - Via dell'De Gasperi, 43 32002 S. Severo - PS</td> <td></td> <td>Per Carico</td> </tr> <tr> <td>2 - Comune di Silea - Via XX settembre, 14 30050 Silea - TV</td> <td>silea.tv@cert.ip-veneto.net</td> <td>Per Carico</td> </tr> <tr> <td>3 - Mazarotto Giancarlo - Via Galileo Galilei, 1 Silea - TV</td> <td>kibernetes_tv@legalmail.it</td> <td>Per Carico</td> </tr> <tr> <td>4 - prefettura di treviso - V. 32</td> <td></td> <td>Per Carico</td> </tr> </tbody> </table>	Destinatari	Email	Tipo invio	1 - Bianchi Mauro - Via dell'De Gasperi, 43 32002 S. Severo - PS		Per Carico	2 - Comune di Silea - Via XX settembre, 14 30050 Silea - TV	silea.tv@cert.ip-veneto.net	Per Carico	3 - Mazarotto Giancarlo - Via Galileo Galilei, 1 Silea - TV	kibernetes_tv@legalmail.it	Per Carico	4 - prefettura di treviso - V. 32		Per Carico
Destinatari	Email	Tipo invio														
1 - Bianchi Mauro - Via dell'De Gasperi, 43 32002 S. Severo - PS		Per Carico														
2 - Comune di Silea - Via XX settembre, 14 30050 Silea - TV	silea.tv@cert.ip-veneto.net	Per Carico														
3 - Mazarotto Giancarlo - Via Galileo Galilei, 1 Silea - TV	kibernetes_tv@legalmail.it	Per Carico														
4 - prefettura di treviso - V. 32		Per Carico														
Titolario d'archivio	3 2															
Descrizione titolario	Titolo 3 / classe 2															
Materia \ Argomento																

La voce **Schemi** consente di creare uno schema predefinito per l'assegnazione automatica di: Titolo, Classe e Sottoclasse.

Le informazioni inserite nei riquadri a fianco sono riprodotte sul protocollo se lo schema di riferimento è quello indicato nella casella della Descrizione.

Figura 16 – Schema protocollo

Dopo aver inserito le informazioni occorre premere sul pulsante **Salva** per renderle disponibili sull'applicativo o sul pulsante **Vai a ..** per uscire senza salvare i dati inseriti.

## 2.8 Note, Note riservate, periodo di pubblicazione, fascioli e relazioni

L'autore di un protocollo può inviare a più destinatari delle note anche riservate scegliendo il pulsante Altri dati (si trova in basso al centro nella finestra di inserimento protocollo). Le note possono essere visibili cioè tutti i destinatari possono leggerle, oppure, possono essere riservate. In questo ultimo caso solo i destinatari abilitati possono leggere le informazioni contenute in esse.

Altri dati protocollo

Salva Chiudi ? help

Estremi fascicolo Documento non inserito in nessun fascicolo

Ricerca fascicolo a cui assegnare UO, oggetto, anno, numero, materia/argomento, intestatario Cerca

Nuovo fascicolo

Materia \ Argomento

Dati registro di emergenza

Codice registro

Anno registro

Numero protocollo

Data protocollo

Dati periodo di conservazione obbligatoria

Anni di conservazione obbligatoria Calcola data

Data scadenza conservazione

Albo pretorio

Riferimento albo pretorio 2012 28

Dati affissione

Data inizio affissione 3 / 12 / 2012

Durata 30

Data fine affissione 02 / 01 / 2013

Calcola data

Tipo documento Avvisi di deposito

Tipo pubblicazione  Integrale  Con omissis

Note

Protocollo in relazione con Cerca in  Affissioni  Appunti  Atti  Documenti

Estendi ricerca per 6 mesi

Cerca

Per estendere la ricerca a tutti i documenti lasciare vuoto (la ricerca sarà estesa a tutti i documenti)

Documenti collegati a questo protocollo

Testo per nota 1

Note riservate 2

Lettori note riservate

Aggiungi Autori del documento

Tramite il campo testo **Note** potranno essere inseriti degli appunti che saranno visibili a tutti i destinatari del protocollo. Utilizzando invece il riquadro **Note riservate** si avrà la possibilità di riservare le annotazioni soltanto ad alcuni destinatari abilitati. Per confermare l'inserimento bisognerà poi trascinare la barra di scorrimento verso l'alto e cliccare quindi sulla voce **Salva**.

Figura 17 - Gestione Note

Nella stessa scheda è possibile indicare il periodo di pubblicazione previsto per il documento oggetto del protocollo.

E' inoltre possibile indicare la natura del documento

**Albo pretorio**

<b>Riferimento albo pretorio</b>	
<b>Dati affissione</b>	Data inizio affissione <input type="text"/> / <input type="text"/> / <input type="text"/> Durata <input type="text"/> Data fine affissione <input type="text"/> / <input type="text"/> / <input type="text"/> <i>Calcola data</i>
<b>Tipo documento</b>	- Nessuno - <input type="button" value="v"/>

A completamento della pubblicazione, nella maschera "Altri dati", sarà riportato il repertorio di pubblicazione associato al protocollo

**Albo pretorio**

<b>Riferimento albo pretorio</b>	2010 102
<b>Dati affissione</b>	Data inizio affissione <input type="text" value="19"/> / <input type="text" value="11"/> / <input type="text" value="2010"/> Durata <input type="text" value="2"/> Data fine affissione <input type="text" value="21"/> / <input type="text" value="11"/> / <input type="text" value="2010"/> <i>Calcola data</i>
<b>Tipo documento</b>	Bandi di gare <input type="button" value="v"/>

E' inoltre possibile assegnare il protocollo ad un fascicolo dalla sezione

**Estremi fascicolo**

Anno	Num.	UO	Oggetto	Titolo/Classe
2012	1	COMUNE D'ITALIA\AFFARI GENERALI	fascicolo per bagnolo	4 / 01/01/2012

Ricerca fascicolo a cui assegnare

sia cercando un fascicolo esistente che creandone uno nuovo tramite la funzione **Nuovo fascicolo**

Quando tutte le informazioni relative al protocollo sono state acquisite, occorre procedere al salvataggio dei dati. L'applicativo provvede così a generare un numero di protocollo e tutti i dati sono registrati in maniera permanente all'interno del sistema (Figura 18).

Oltre alla fascicolazione è possibile collegare il protocollo con qualsiasi altro oggetto all'interno del programma utilizzando la funzione di "relazione"

**Protocollo in relazione con**

Cerca in  Affissioni  Appunti  Atti  Documenti  Proposte  Protocolli  Sedute

Estendi ricerca per  mesi

*Per estendere la ricerca a tutti i documenti lasciare vuoto (la ricerca potrebbe durare molto tempo)*

La funzione presenta inizialmente una condizione neutra dove l'utente deve dire, cliccando sulle apposite funzioni **Cerca in**  Affissioni  Appunti  Atti  Documenti  Proposte  Protocolli  Sedute , in quale archivio è presente il documento in relazione con il protocollo.

Una volta definiti i criteri di ricerca e cliccato su **Cerca** i risultati di una ricerca vengono presentati in un elenco

	Tipo atto	UO	Anno	Numero	Oggetto
<input type="checkbox"/>	determinazione del 1° settore	COMUNE D'ITALIA\ECONOMICO - FINANZIARIO	2011	11	Atto di indirizzo per il computo dei limiti di spesa giornalieri nelle trasferte
<input type="checkbox"/>	determinazione del 1° settore	COMUNE D'ITALIA\ECONOMICO - FINANZIARIO	2011	8	Oggetto dell'atto
<input type="checkbox"/>	determinazione del 1° settore	COMUNE D'ITALIA\1° SETTORE RAPPORTI CON GLI ORGANI COLLEGIALI	2011	5	oggetto dell'atto
<input type="checkbox"/>	determinazione del 1° settore	COMUNE D'ITALIA\AFFARI GENERALI\PROTOCOLLO E URP\Servizi Polivalenti	2011	4	oggetto dell'atto
<input type="checkbox"/>	determinazione del 3° settore	COMUNE D'ITALIA\AFFARI GENERALI	2011	2	atto di test
<input type="checkbox"/>	determinazioni del 2° settore	COMUNE D'ITALIA\ECONOMICO - FINANZIARIO	2011	1	Oggetto dell'atto

E' possibile selezionare uno o più documenti da porre in relazione semplicemente cliccando sul riquadro .

L'operazione si conclude cliccando su "Ok" o "Chiudi"

Ad operazione conclusa, i documenti selezionati vengono descritti come in relazione con il protocollo corrente

Documenti collegati a questo protocollo			
	Tipo doc.	Estremi	Oggetto
<input type="checkbox"/>	Atto	2012 3	OGGETTO DELLA DETERMINA!!

Una volta compilato il protocollo in tutte le sue parti cliccando su **Salva** nella maschera principale, ci verrà restituito il numero di protocollo in una pop up

Chiudi	Stampa segnatura	Stampa etichette	Stampa ricevuta
--------	---------------------	---------------------	--------------------

**Protocollo numero 69 del 27/5/2011 inserito**

**Figura 18** - Numero Protocollo

Abbiamo così visto tutte le operazioni necessarie per creare un protocollo. La figura rappresenta la schermata iniziale di un protocollo "a regime" quando cioè sono state raccolte e registrate una quantità considerevole di dati. Come si può notare nella figura, alcune informazioni di riepilogo sono contenute nella schermata iniziale.

	2011 91	27/9/2011	Invio comunicazioni Capigruppo U.O.R: COMUNE D'ITALIA\AFFARI G Intestatari: Albini Andrea
	2011 90	26/9/2011	soggetti inseriti a mano U.O.R: COMUNE D'ITALIA\AFFARI G Intestatari: Perillo Marco
	2011 89	26/9/2011	comunicazione capigruppo U.O.R: Intestatari: Albini Andrea
	2011 88	8/9/2011	Tende VELUX: risparmio con la soluzione Progetti e Oscura - Libero Spot U.O.R: COMUNE D'ITALIA\AFFARI GENERALI
	2011 87	8/9/2011	
	2011 86	7/9/2011	
	2011 85	7/9/2011	Tende VELUX: risparmio con la soluzione Progetti e Oscura - Libero Spot U.O.R: COMUNE D'ITALIA\AFFARI GENERALI\UO2 Intestatari: Marco Perillo

Il protocollo in **entrata** è indicato con una freccia rossa, quello in **uscita** con una freccia verde, quello **interno** con una freccia azzurra.

Sulla stessa riga sono visualizzate le informazioni obbligatorie:

1. **Entrata/Uscita/Interno**
2. **Numero Protocollo**
3. **Data**
4. **Oggetto**
5. **UO**

Alle informazioni in elenco sono affiancate varie giff con l'obbiettivo di rendere più rapida e completa la consultazione delle informazioni di protocollo.

- = protocollo pubblicato all'albo pretorio
- = protocollo proveniente da posta istituzionale
- = protocollo proveniente da posta certificata
- = protocollo inoltrato tramite posta certificata
- = protocollo contenente allegati firmati digitalmente
- / = protocollo inserito in un fascicolo / subfascicolo
- = protocollo annullato
- = protocollo riservato
- = presenza di documenti allegati al protocollo
- = accesso rapido in modifica del protocollo
- = presenza ulteriori mittenti/destinatari oltre a quelli visualizzati in elenco

Oltre alle informazioni obbligatorie, la pagina iniziale del protocollo contiene altre indicazioni. Ad esempio se il protocollo è stato annullato oppure se è riservato.

È utile precisare che tutte le informazioni non obbligatorie inserite possono essere modificate (dagli aventi diritto). Tutte le modifiche vengono però "tracciate" nel senso che il sistema indica chi ha modificato le informazioni, come indicato dal D.P.C.M. del 31 Ottobre 2000 all'art. 8 comma 2, che riporta:

*...“Delle altre informazioni, registrate in forma non modificabile, l’annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l’ora e all’autore della modifica; così analogamente per lo stesso campo, ad ogni altro, che dovesse poi risultare errato”.*



## 2.9 Riservatezza

Nel paragrafo precedente è stata commentata la funzionalità relativa alla riservatezza del protocollo. Tuttavia, nessuna delle informazioni fino ad ora inserite consente di rendere il protocollo riservato. Alcune funzionalità possono essere abilitate solamente quando il protocollo è stato salvato, la riservatezza è tra queste.

Per attivare tali funzionalità occorre aprire il protocollo già registrato e cliccare sul pulsante “Modifica” (vedi Figura 19).



Figura 19 - Modifica Protocollo

Dopo di che si possono effettuare delle funzionalità aggiuntive, in particolare:

1. Rendi Riservato
2. Annulla
3. Stampa ricevuta
4. Crea susseguente

## 5. Crea copia

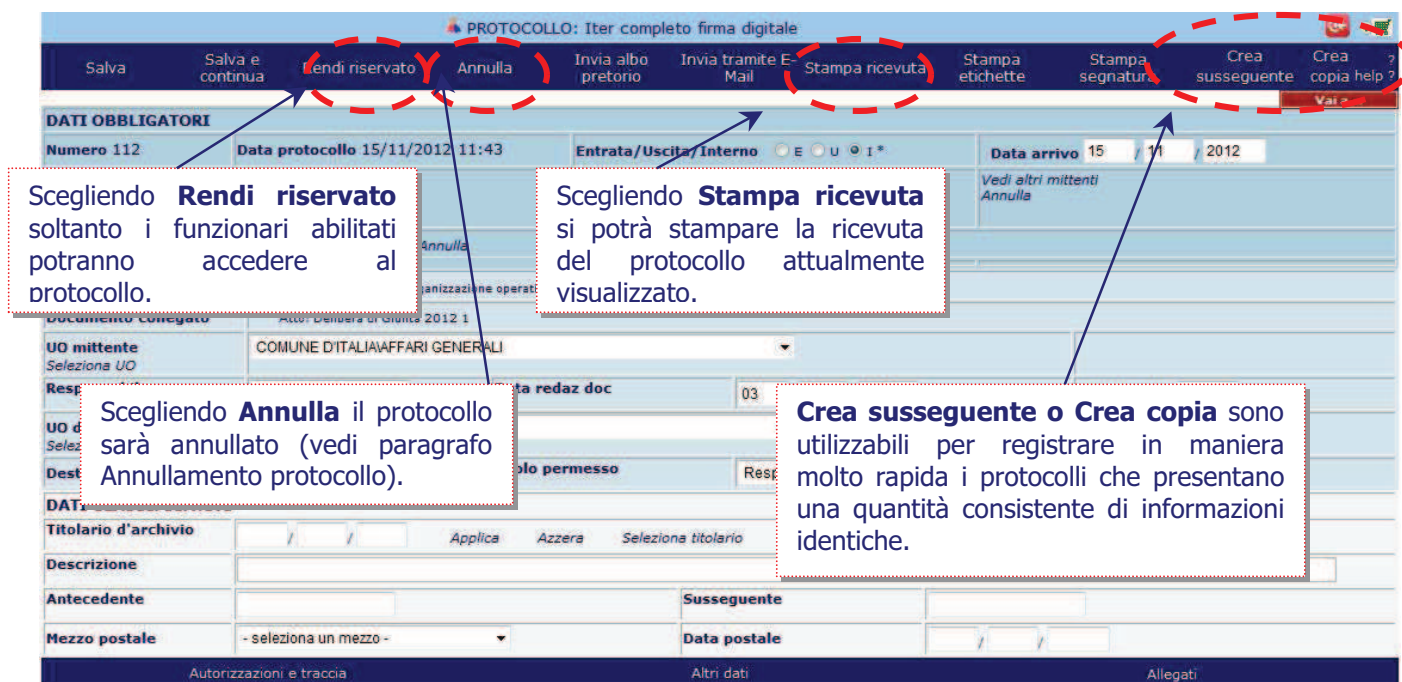


Figura 20 - Modifica Protocollo

Le funzionalità aggiuntive sopra indicate sono disciplinate dal D.P.C.M. del 31 ottobre 2000 sulla base di quanto disposto dall'art. 53 comma 4 del citato D.P.R. 445/2000.

L'applicativo è sviluppato in armonia con le regole tecniche imposte dalla normativa.

Per rendere riservato il protocollo è sufficiente cliccare in corrispondenza del pulsante "Rendi Riservato" (Figura 20). Dopo di che si selezionano i funzionari abilitati a leggere le informazioni contenute e successivamente si seleziona il pulsante "Rendi riservato" (Figura 21).

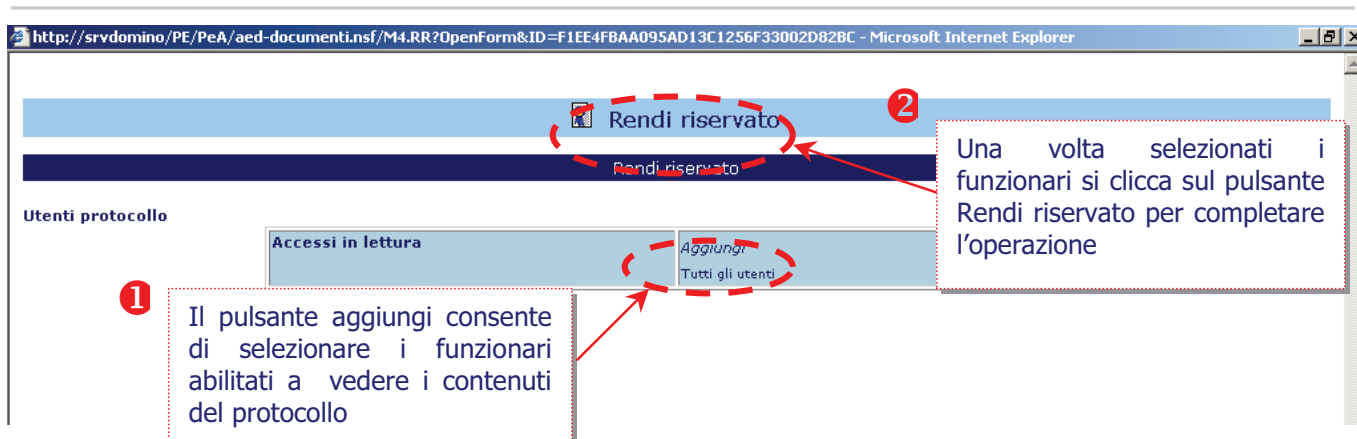


Figura 21 – Rendi riservato

Per togliere la riservatezza la procedura è identica. L'applicativo riconosce che il protocollo è riservato e sulla barra dei pulsanti renderà disponibile al posto di "Rendi Riservato", l'opzione "Togli Riservatezza" (Figura 22).

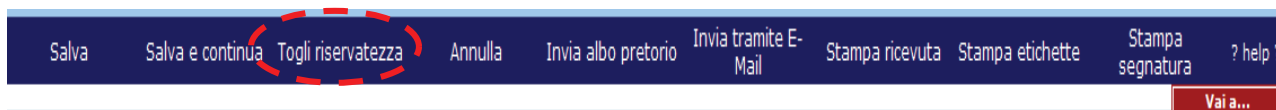
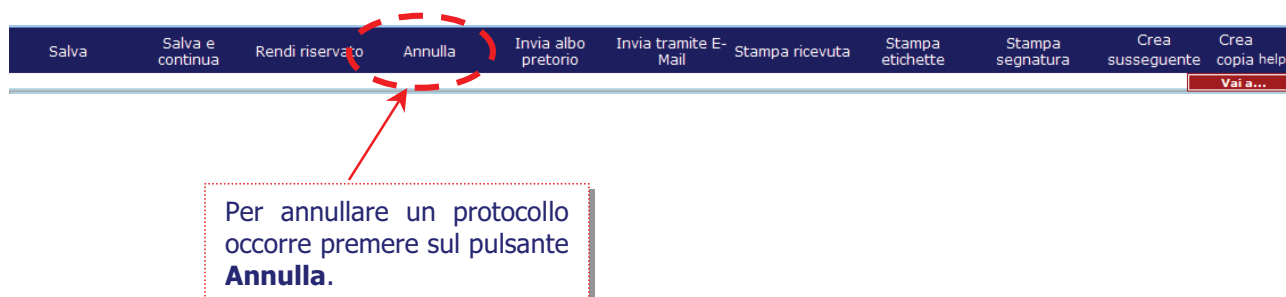


Figura 22 - Togli riservatezza

L'applicativo consente di annullare la riservatezza al documento protocollato cliccando sulla funzione **Togli riservatezza**.

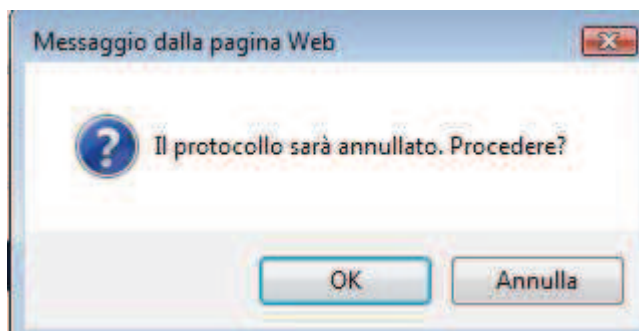
## 2.10 Annullamento Protocollo

Le operazioni che si rendono necessarie per annullare un protocollo sono simili a quelle utilizzate nei due esempi precedenti, si apre cioè un protocollo precedentemente registrato, si seleziona il pulsante “Modifica” (Figura 19) e successivamente si clicca sul pulsante “Annulla” (Figura 23).



**Figura 23** - Annullamento Protocollo

L’abilitazione all’operazione di annullamento è assegnata solamente al gestore del protocollo. Tutti gli altri utenti non hanno la possibilità di operare con questa funzionalità. Tuttavia, essendo una operazione irreversibile, il sistema chiede una conferma dell’operazione attraverso il message box visualizzato in Figura 24.



**Figura 24** - Annullamento Protocollo

Una volta che il responsabile ha dato conferma premendo sul pulsante OK, il protocollo viene annullato e una croce rossa viene visualizzata sulla schermata iniziale del PROTOCOLLO. L’annullamento non implica, come già sottolineato, la perdita dei dati del protocollo i quali rimarranno sempre residenti sul sistema. Queste funzionalità sono conformi a quanto disposto dall’art.5, comma 1 del decreto del Presidente della Repubblica n. 428/1998 che testualmente cita:

*...“Le informazioni annullate, in conformità alle disposizioni del presente regolamento, devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. La procedura per indicare l’annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie, poi annullate, unitamente alla data, all’identificativo dell’operatore ed agli estremi del provvedimento d’autorizzazione”.*

## 2.11 Stampa ricevuta

Per rilasciare agli utenti la ricevuta cartacea di avvenuta protocollazione bisogna cliccare sulla voce **Stampa ricevuta** (Figura 25 – **Stampa ricevuta**) dopodichè si avvierà una procedura guidata che ci consentirà di ottenere facilmente la ricevuta del documento .



Figura 25 – Stampa ricevuta

Scegliendo **Stampa ricevuta** si potrà stampare la ricevuta del protocollo attualmente visualizzato.

PROTOCOLLO: Iter completo firma digitale

Salva Salva e continua Rendi riservato Annulla Invia albo pretorio Invia tramite E-Mail **Stampa ricevuta** Stampa etichette Stampa segnatura Crea susseguente Crea copia help ? Vai a...

**DATI OBBLIGATORI**

Numero 112 Data protocollo 15/11/2012 11:43 Entrata/Uscita/Interno  E  U  I\* Data arrivo 15 / 11 / 2012

Mittente Ragione sociale Kibernetes Indirizzo Via di Kibernetes, Nr. 1/1 Scala 1 Int. 1 12345 Città di Kibernetes TV Vedi altri mittenti Annulla

Oggetto Iter completo firma digitale Annulla

**RIFERIMENTI E DESTINATARI INTERNI**  Organizzazione operativa  Organizzazione politica

Documento collegato Atto: Delibera di Giunta 2012 1

UO mittente Seleziona UO COMUNE D'ITALIA AFFARI GENERALI

Responsabile Perillo Marco Data redaz doc 03 / 02 / 2012

UO destinataria Seleziona UO sponsabile Area Affari Generali

Destinatario - Nessuno - Ruolo permesso Responsabile Area Affari Generali

**DATI CLASSIFICATIVI**

Titolario d'archivio / / Applica Azzera Seleziona titolare

Descrizione

Antecedente Susseguente

Mezzo postale - seleziona un mezzo - Data postale / /

Autonizzazioni e traccia Altri dati Allegati

Tutti i dati inseriti sono riprodotti in modalità modifica nel senso cioè, che il protocollista può cambiare solamente le informazioni che risultano differenti.

Figura 26 - Crea susseguente

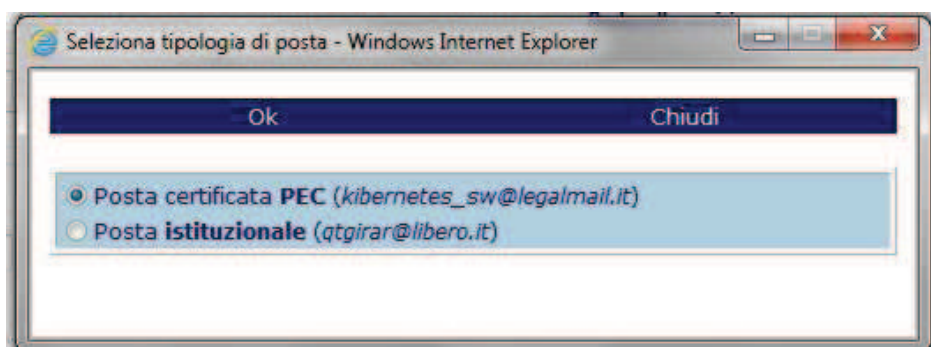
## 2.12 Invia tramite mail

La funzione è denominata **Invia tramite E-Mail**, consente sia di inviare una mail “formale” e quindi utilizzando l’indirizzo PEC dell’ente, sia di inviare una mail “informale” utilizzando quindi l’indirizzo di posta istituzionale” o comunque il primo indirizzo descritto in -> “AMMINISTRAZIONE ->Configurazione -> Parametri”, nella sezione “Modulo protocollo” alla voce

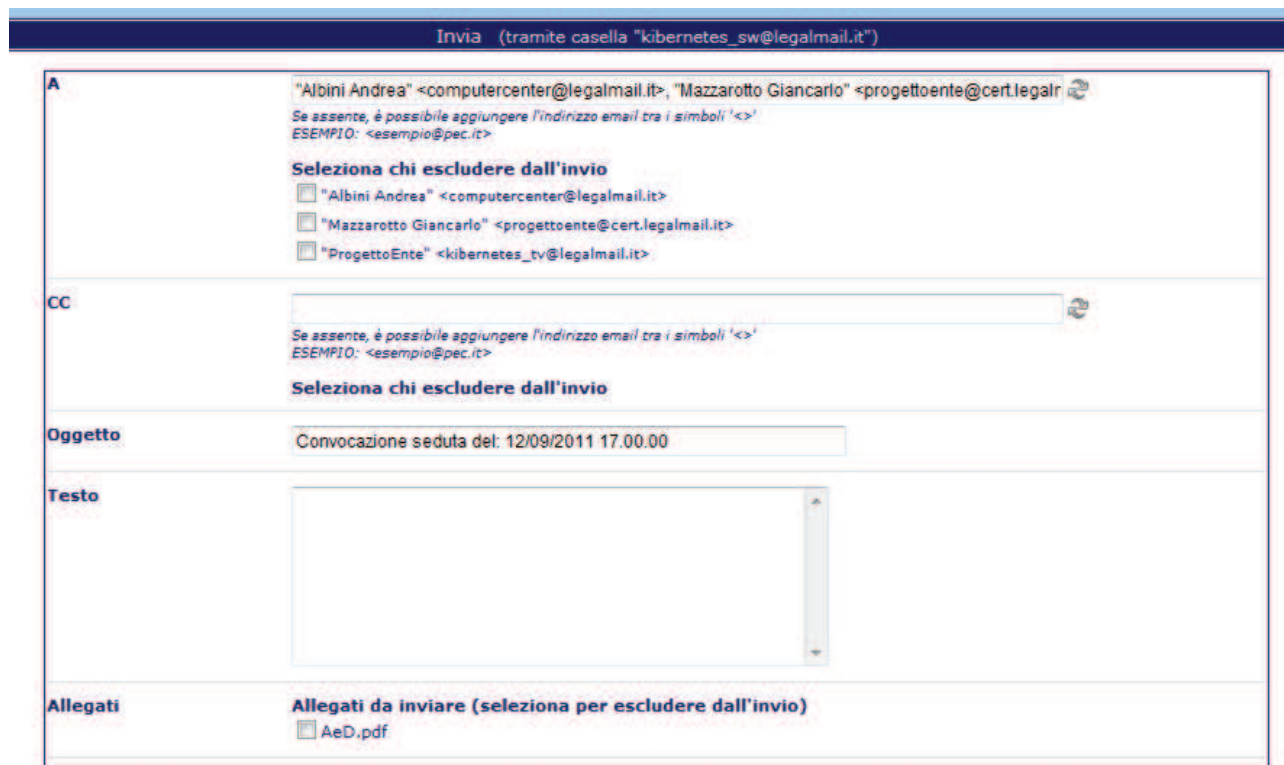
Specificare l'indirizzo certificato di posta elettronica del protocollo

Specificare gli indirizzi di posta elettronica istituzionale (separati da virgola)

Cliccando su “Invia tramite E-mail” appare un box dove si chiede attraverso quale indirizzo di posta si intende spedire il documento



Scelto l’indirizzo, cliccando su “Ok” l’applicativo presenta una maschera di invio posta del tipo riportata in figura





dove:

Viene specificato quale indirizzo è stato scelto **Invia** (tramite casella "kibernetes\_sw@legalmail.it")

Vengono proposti automaticamente tutti i destinatari. Sarà comunque sempre possibile aggiungere destinatari secondo le modalità consuete e descritte nel messaggio di aiuto

*Se assente, è possibile aggiungere l'indirizzo email tra i simboli '<>'*  
ESEMPIO: <esempio@pec.it>

E' possibile escludere dall'invio alcuni soggetti ( esempio perché interessati al documento ma privi di posta elettronica o non interessati a questa specifica fase documentale ) semplicemente cliccando su check box alla sinistra di ogni interessato

**Selezione chi escludere dall'invio**

- "Albini Andrea" <computercenter@legalmail.it>
- "Mazzarotto Giancarlo" <progettoente@cert.legalmail.it>
- "ProgettoEnte" <kibernetes\_tv@legalmail.it>

Deselezionando uno o più destinatari, automaticamente viene aggiornato l'elenco dei destinatari



E' consentita la manutenzione dell'oggetto che verrà presentato come oggetto della mail in arrivo

E' consentito inserire un testo che sarà presentato come corpo di mail ai destinatari del documento

E' consentito deselezionare uno o più allegati ( nel caso di vogliono mandare solo parte del documento ) semplicemente cliccando sul riquadro relativo all'allegato che non si desidera inviare



- a) Ad ogni invio, viene tracciato chi ha spedito e come ( posta certificata o istituzionale ), cosa è stato spedito e i destinatari dei documenti.

**TRACCIA INVIO TRAMITE EMAIL**

• In data 17/11/2011 alle ore 14:03:22 l'operatore Alessandro Bianchi ha inviato a "vari cittadini" <>, "gazzettino" <bonettol@libero.it> previo la casella email qtgirar@libero.it  
Testo: si inoltra il presente documento perché ne venga data diffusione. distinti saluti  
Allegati AeD.pdf.p7m

La funzione **Invia tramite E-Mail** è sempre attiva consentendo quindi di inviare lo stesso documento più volte a seconda, ad esempio, dello stato di avanzamento o inviando selettivamente alcuni allegati solo a specifici destinatari.

## 2.13 Crea susseguente

La funzionalità crea susseguente si rende necessaria per registrare in maniera molto rapida i protocolli che presentano una quantità consistente di informazioni identiche.

Per attivare la funzionalità occorre selezionare il pulsante “Modifica” (Figura 19) in corrispondenza del protocollo sul quale si intende creare una copia. Successivamente (vedi Figura 20) si clicca sul pulsante “Crea susseguente”. Un protocollo con le informazioni già registrate viene visualizzato come in Figura 26 - **Crea** in cui i campi sono però modificabili. Questa funzionalità è resa necessaria per garantire al protocollista di cambiare alcune delle informazioni precedentemente inserite e lasciare inalterate quelle che non hanno bisogno di essere modificate. Da notare che l'applicativo indica cronologicamente le eventuali relazioni che si susseguono tra protocolli nei quali si è utilizzata (anche ripetutamente) la funzione **Crea susseguente/Copia**, visualizzando nel campo antecedente gli eventuali collegamenti con protocolli precedentemente immessi e in quello susseguente i rapporti con quelli protocollati successivamente .

Per creare una copia e assegnare un numero di protocollo è sufficiente cliccare in corrispondenza del pulsante “Salva ed esci”. Il pulsante “Vai a ..” consente invece, di uscire dalla modalità crea susseguente senza salvare le informazioni, cioè senza generare il numero di protocollo.

Sempre nell'ottica di semplificare e velocizzare le operazioni di protocollazione, sono state introdotte delle funzioni nel processo di "Copia da protocollo" presente nella maschera di un nuovo protocollo.

Copia da protocollo (Anno/Nr.)  /  *Sussequente Copia*

La funzione consente di creare nuovi protocolli copiando i contenuti da un protocollo già in archivio. Non sempre però si conosce il numero di protocollo dal quale si vuole copiare il contenuto.

La funzione introdotta consente di cercare il protocollo da copiare durante le operazioni di "Copia" o "Sussequente".

Nel dettaglio, se non si conoscono gli estremi "Anno/Numero", lasciando tali campi in bianco, sarà possibile, cliccando su "Sussequente" o "Copia", attivare una funzione di ricerca di tipo "QBE" limitata ai campi che più frequentemente sono utilizzati per le ricerche.








Cerca

 Ricerca su protocolli per copia/sussequente

Tipo ricerca	<input checked="" type="radio"/> AND <input type="radio"/> OR	
Anno Protocollo	dal 2010	al <input type="text"/>
Numero Protocollo	dal <input type="text"/>	al <input type="text"/>
Data Protocollo	dal <input type="text"/> / <input type="text"/> / <input type="text"/> al <input type="text"/> / <input type="text"/> / <input type="text"/>	
E/U/I	- Nessuna - <input type="button" value="v"/>	
Intestatario	<input type="text"/>	
Altri intestatari	<input type="text"/>	
Oggetto	<input type="text"/>	
Ordine	Ordinamento vista <input type="button" value="v"/>	
Quanti risultati	Tutti <input type="button" value="v"/>	

Sarà quindi possibile impostare la ricerca

[Visualizza criterio di ricerca](#) [? help ?](#)

	Anno num	Data	Oggetto	UO	Intestatari
<b>Trovati 15 protocolli con criterio di ricerca specificato</b>					
		2010 15	13/4/2010	richiesta adesione a manifestazione del "Comune in fiore"	COMUNE D'ITALIA\AFFARI GENERALI Bianchi Mauro
		2010 14	2/4/2010	test permessi estesi a ruolo permesso	COMUNE D'ITALIA\AFFARI GENERALI Albini Andrea
		2010 13	23/3/2010	test numero 3	COMUNE D'ITALIA\ECONOMICO - FINANZIARIO comune di pescantina
		2010 12	23/3/2010	test numero 2	COMUNE D'ITALIA\AFFARI GENERALI Bianchi Mauro
		2010 11	23/3/2010	oggetto 1 per verifica permessi a ruoli	COMUNE D'ITALIA\AFFARI GENERALI città di venezia
		2010 10	17/3/2010	oggetto del documento da protocollare e successivamente da inviare all'albo pretorio	COMUNE D'ITALIA\AFFARI GENERALI Albertini Stefano

e, selezionando il risultato desiderato, pre caricare il nuovo protocollo come "Sussequente" o "Copia".

### 3 FUNZIONE CERCA

Una funzionalità particolarmente interessante implementata nell'applicativo è quella relativa alla possibilità di ricercare nell'archivio un determinato protocollo sulla base di alcune o molte informazioni fornite dall'utente. È evidente che tanto più accurata è stata la raccolta delle informazioni in fase di input e tanto più efficace e veloce risulta l'individuazione del protocollo di riferimento.



Figura 27 - Ricerca Testuale

L'applicativo fornisce tre modalità di ricerca (Figura 27 - Ricerca Testuale). La **prima** è una ricerca in base al numero di protocollo, la **seconda** e la **terza**, descritte nel successivo paragrafo, sono invece delle ricerche testuali in base ad un testo, ad una parola chiave o ad altri parametri forniti dall'utente. Per accedere al motore di ricerca testuale è sufficiente cliccare in corrispondenza dei pulsanti evidenziati in Figura 27.



Figura 28 - Ricerca Testuale

Come si può notare in Figura 28, le informazioni necessarie alla **seconda ricerca** per generare dei risultati sono:

- a)** Digita il testo da ricercare;
- b)** Ordine (indica se i dati devono essere visualizzati in ordine crescente di data o in ordine decrescente di data);
- c)** Quanti risultati (indica la numerosità di dati visualizzati in ogni schermata, le opzioni disponibili sono: Tutti, 10, 20, 50 e 100).

Dopo aver inserito le informazioni necessarie, l'operatore procede a cliccare sul pulsante "Cerca" per attivare la ricerca.

Premendo il pulsante "Vai a ..", il sistema non produce nessun risultato ma esce dalla modalità ricerca per ritornare sulla schermata iniziale del protocollo.

La **terza modalità di ricerca** (vedi Figura 29), è puntuale, nel senso che l'operatore indica in corrispondenza di ogni singolo campo del protocollo le informazioni sulle quali intende produrre dei risultati, per attivarla occorre selezionare il pulsante indicato in Figura 27.

Utilizzando la terza modalità di ricerca i risultati generati dal motore di ricerca sono decisamente inferiori a quelli prodotti secondo la prima metodologia, e pertanto la possibilità di rintracciare in maniera più rapida il protocollo desiderato sono superiori.

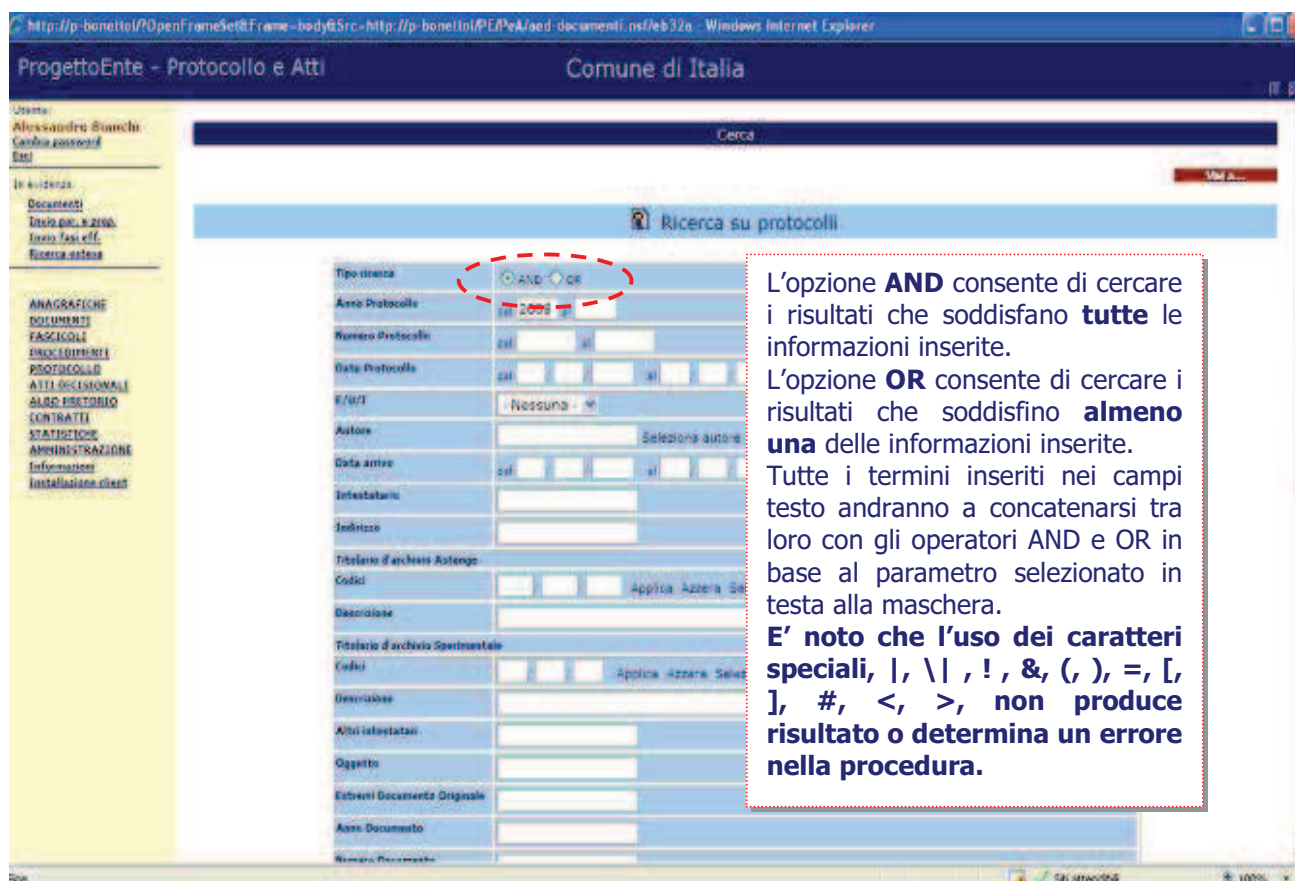


Figura 29 - Ricerca Puntuale

Una precisazione ulteriore merita la funzione “AND” o “OR”.

L'opzione “AND” consente di cercare i risultati che soddisfano contemporaneamente tutte le informazioni inserite dall'operatore.

L'opzione “OR” consente di cercare i risultati che soddisfano almeno una delle informazioni inserite dall'operatore.

Analogamente al caso precedente per attivare la funzione di ricerca occorre premere sul pulsante “Cerca” oppure su “Vai a ..” se non si intende attivare nessuna ricerca. L'applicativo in questo secondo caso ritorna sulla posizione iniziale rappresentata dalla schermata iniziale del protocollo.



## 4 REGISTRO D'EMERGENZA

La normativa vigente, come sancito dall'art. 63 del D.P.R. 445/2000<sup>1</sup>, prevede che in caso di arresto delle funzionalità del protocollo informatico (guasto tecnico, black out, ecc..) l'ufficio di protocollo è tenuto a dare continuità alla sua funzione amministrativa facendo ricorso ad un registro d'emergenza cartaceo con il quale gestire il protocollo fino al completo ripristino delle funzionalità del sistema elettronico.

A sistema di protocollazione elettronica ristabilito bisogna reinserire cronologicamente in ordine ascendente i protocolli del registro d'emergenza utilizzando la funzione Nuovo Protocollo. All'apertura della relativa finestra (Figura 3) bisogna, documento per documento, completare i vari campi fino a raggiungere la parte inferiore della finestra e cliccare sul pulsante Altri dati (Figura 33) dopodichè si aprirà un'altra piccola finestra in cui alla voce **Dati registro di emergenza** vanno inseriti:

1. Codice registro (il codice univoco del registro di emergenza, es. R.E.);
2. Anno registro (quello corrente);
3. Numero protocollo, come da registro d'emergenza;
4. Data protocollo (gg/mm/aaaa), come da registro d'emergenza.

Infine bisogna confermare con Salva e quindi scegliere di salvare anche il protocollo.

---

<sup>1</sup> **Articolo 63 del D.P.R. 445/2000** ("Registro di emergenza")

**1.** Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

**2.** Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione.

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

**4.** La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.

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

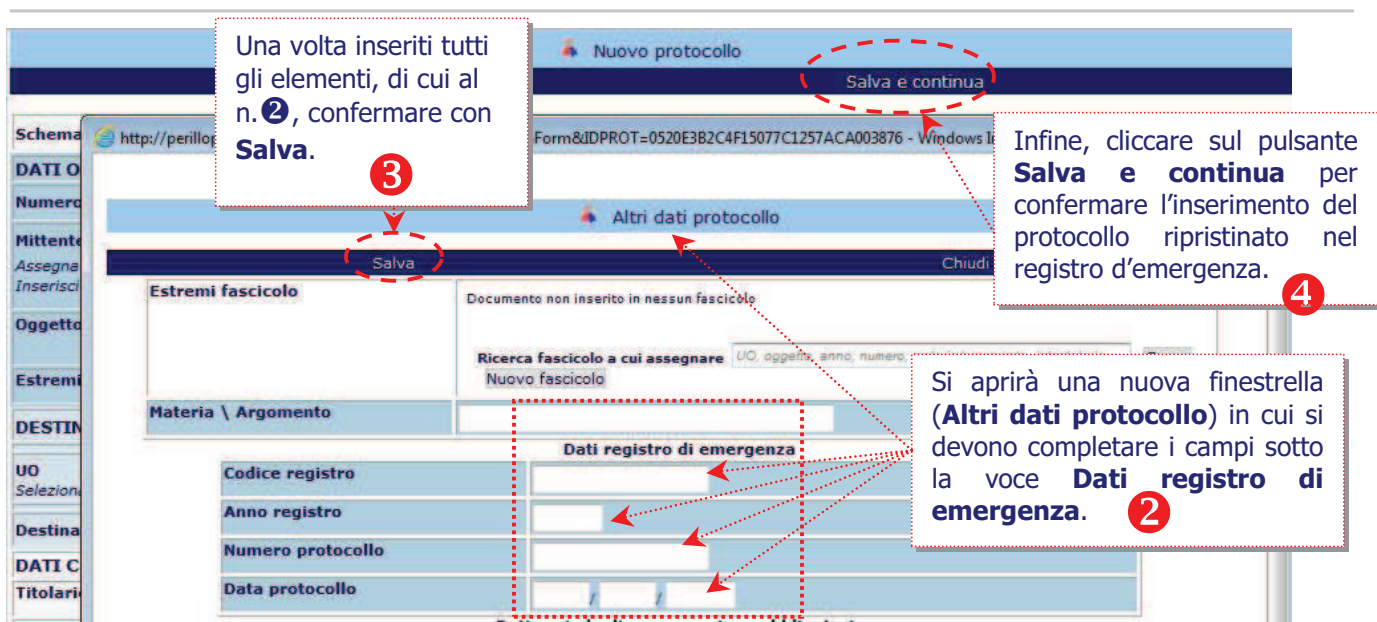


Figura 30 – Registro di emergenza

Dopo aver inserito tutti i dati nella finestra Nuovo protocollo, cliccare in basso sulla voce **Altri dati**. **1**

## 5 STAMPA DEI REGISTRI

1) **Stampa Registro Protocollo**: è una funzione che consente di riprodurre in forma cartacea i protocolli informatici acquisiti dal sistema e presenti nell'archivio elettronico.



**Figura 31** - Stampa Registro

Questa funzionalità può essere utilizzata in diverse modalità a seconda delle esigenze amministrative. La prima che andremo a vedere riguarda la “Stampa del Registro Protocollo” che si attiva cliccando sul pulsante corrispondente come visualizzato in Figura 31.

In base alla modalità utilizzata saranno applicati diversi filtri che consentiranno una stampa in base a:

- L'anno;
- La data del protocollo;
- Il numero del protocollo;
- Protocollo in entrata - uscita, entrata, uscita, interno.

Vediamo, adesso, una ad una le singole modalità:

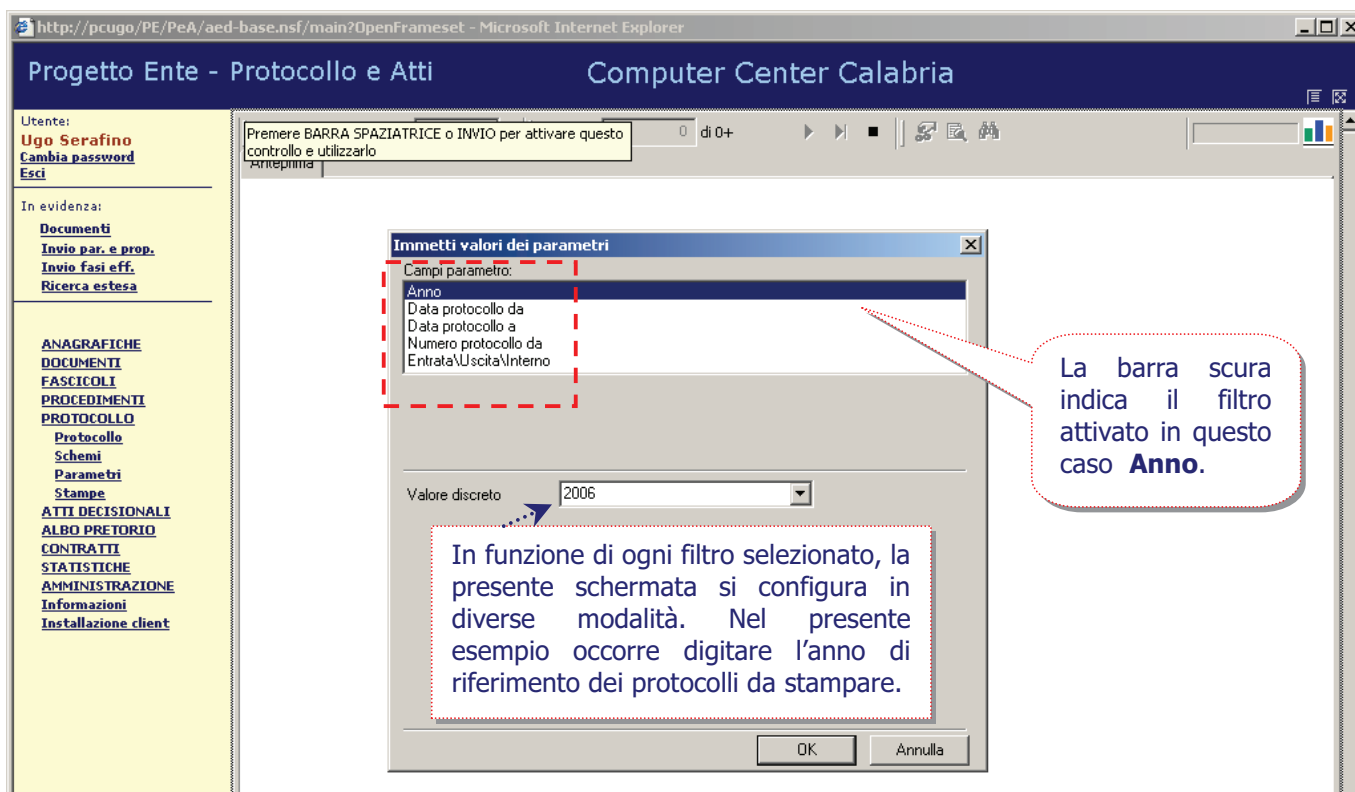


Figura 32 - Stampa Registro

a) **Stampa per anno:** dopo aver selezionato il parametro anno (come in Figura 32 - **Stampa Registro**), inserire l'anno, ad esempio 2004, nel campo Discrete Value (Valore discreto) e quindi cliccare su OK.

b) **Stampa per data:** per stampare i protocolli effettuati in una determinata data, o in un determinato periodo, l'opzione che occorre scegliere è quella rappresentata da "Data protocollo (nella forma da/a)" come raffigurato in Figura 33. Rispetto al caso precedente nel quale era sufficiente indicare l'anno di riferimento per ottenere i risultati, in questo caso ci sono delle quantità maggiori di opzioni da indicare. Se ad esempio, l'ufficio protocollo intende stampare i protocolli che vanno dallo 01/01/2006 al 15/08/2006, deve indicare in corrispondenza di **Data protocollo da** (vedi Figura 33) la data iniziale ed in corrispondenza di **Data protocollo a** la data finale, sempre espresse nel formato gg/mm/aaaa, dopodichè bisogna cliccare su **OK** per confermare la scelta, a video apparirà un elenco cronologico e stampabile dei protocolli interessati nella ricerca.

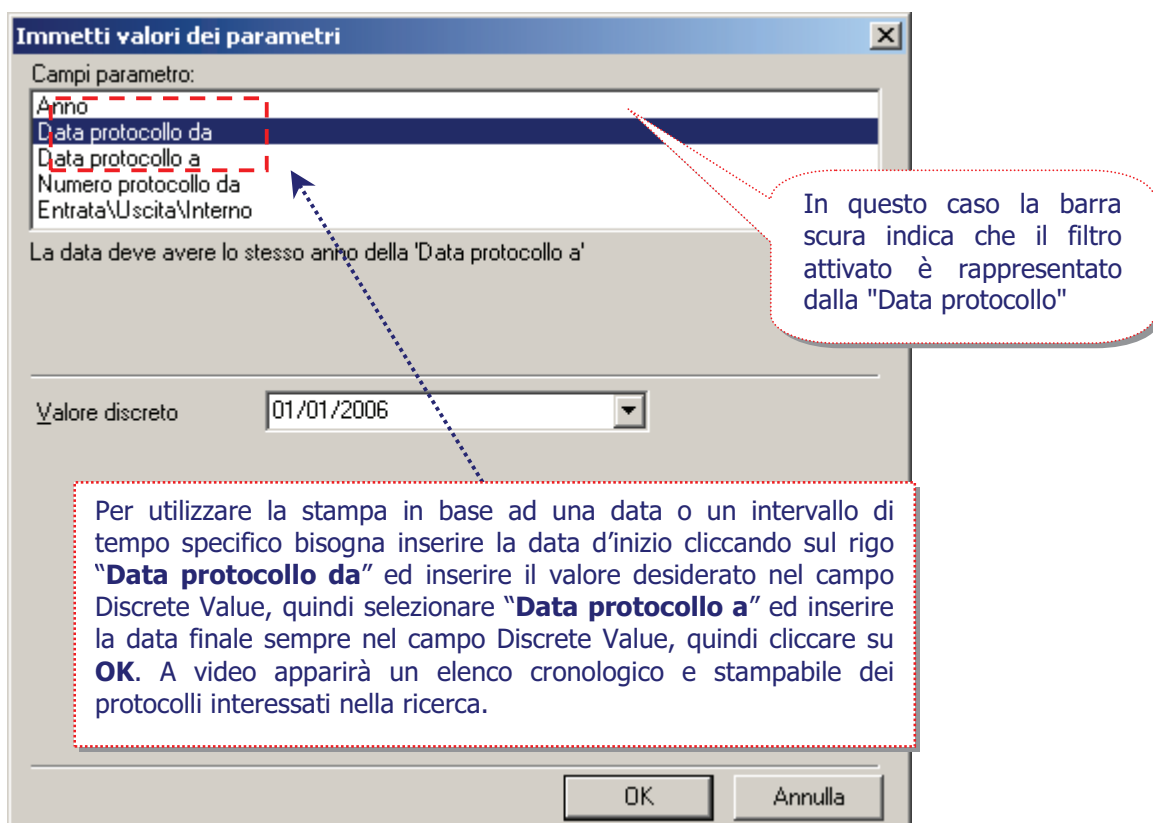


Figura 33 - Stampa Registro

c) **Stampa per numero protocollo:** Il terzo filtro utilizzabile è strutturato in funzione del numero di protocollo. Come visualizzato in Figura 34, nel campo corrispondente a “Discrete Value”, viene inserito il numero di protocollo a partire dal quale si intende stampare i dati.

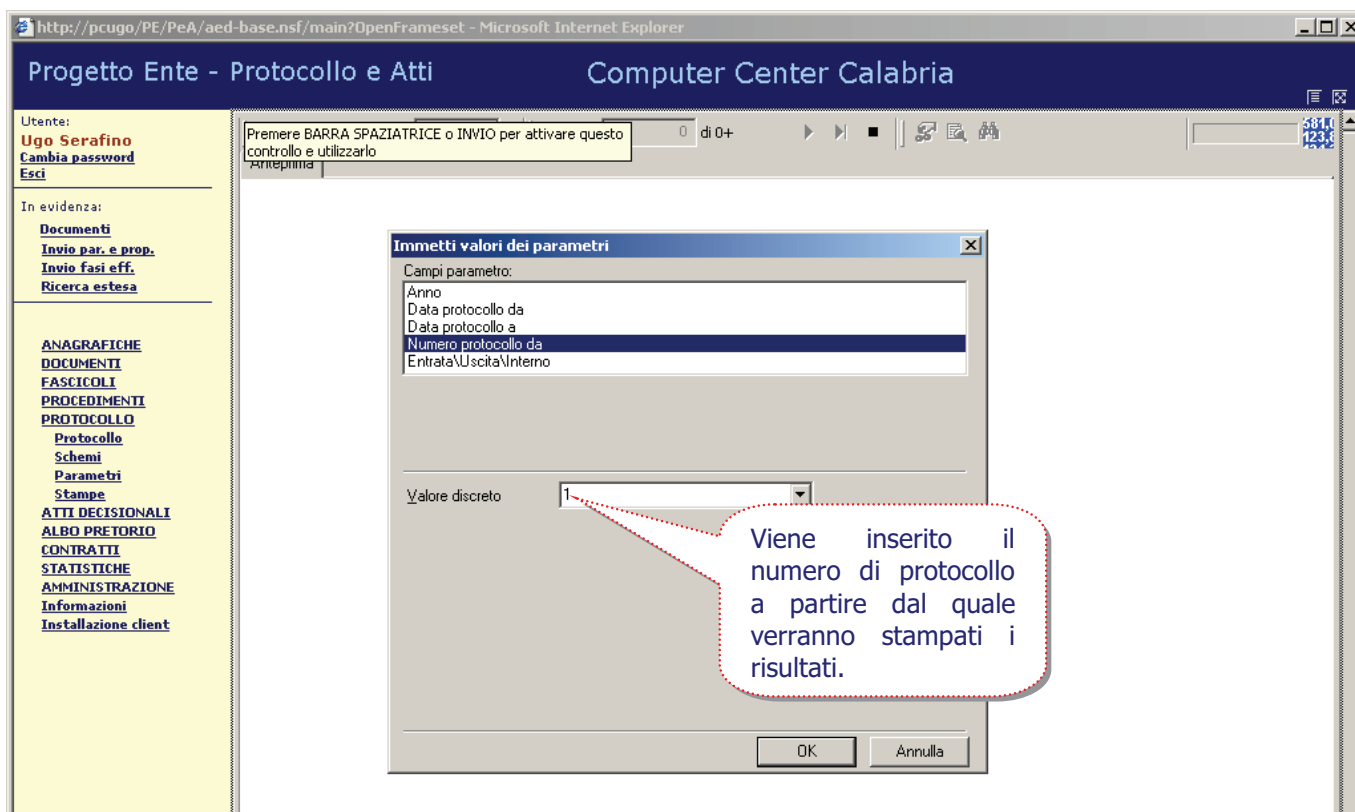


Figura 34 - Stampa Registro

d) **Stampa per protocollo in Entrata/Uscita/Interno:** L'ultima modalità di funzionamento del filtro è quella relativa ai protocolli in Ingresso, Uscita e Interno dell'Ente. Così come si è visto negli esempi precedenti, è sufficiente selezionare l'opzione desiderata (vedi Figura 35) e cliccare sul pulsante OK per confermare la scelta e procedere alla stampa.



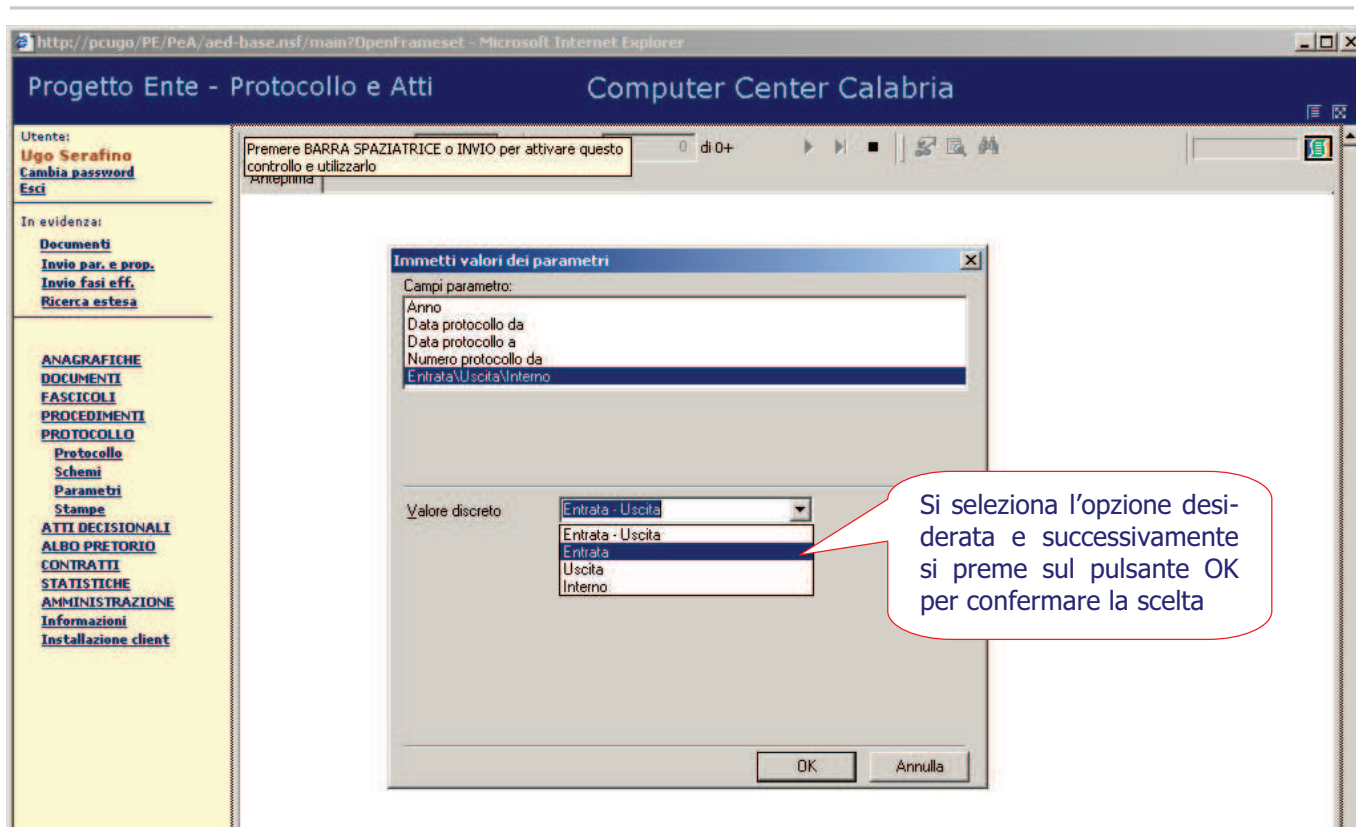
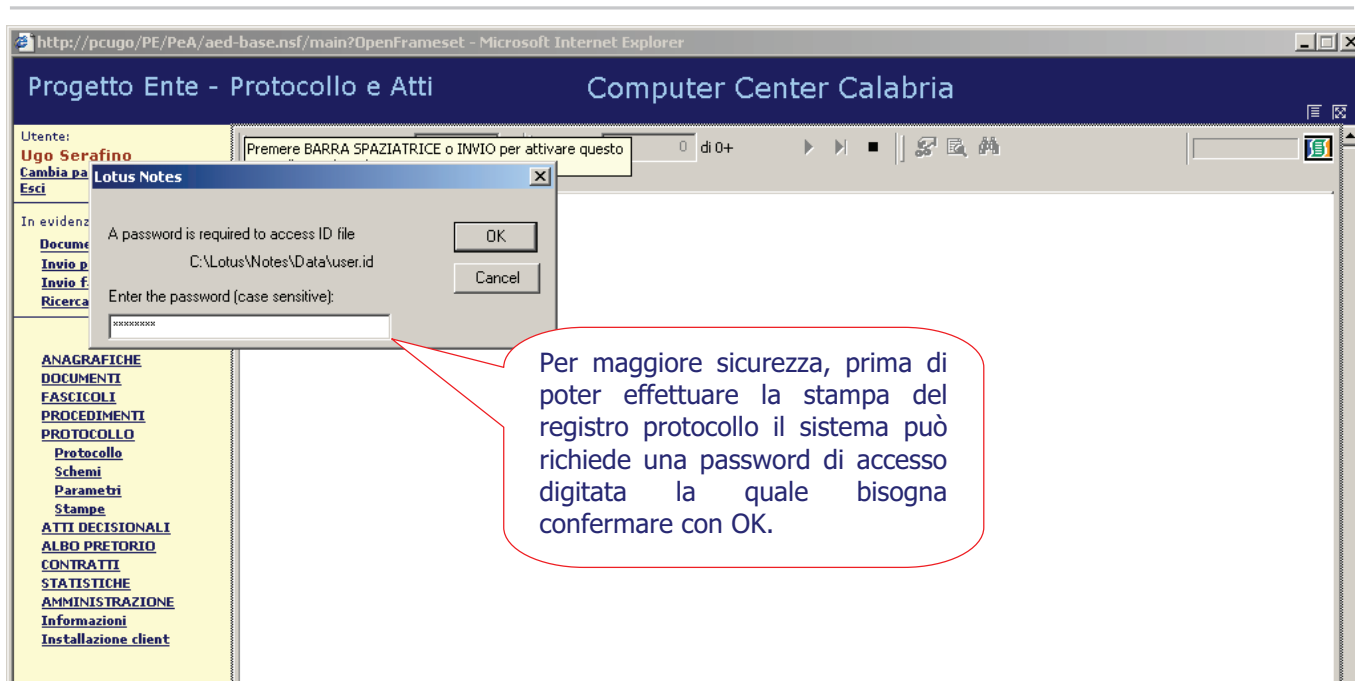


Figura 35 - Stampa Registro

Una volta selezionata la tipologia del filtro secondo le suddette modalità e aver confermato con "OK", il sistema può chiedere l'inserimento della password (Figura 36) al fine di evitare che utenti non abilitati alla funzione possano accedervi. I dati vengono quindi visualizzati sullo schermo secondo i criteri del filtro precedentemente adottati.



**Figura 36 - Stampa Registro**

I dati sono visualizzati in anteprima sullo schermo (Figura 37) e, attraverso la barra degli strumenti diventa possibile effettuare ulteriori personalizzazioni.

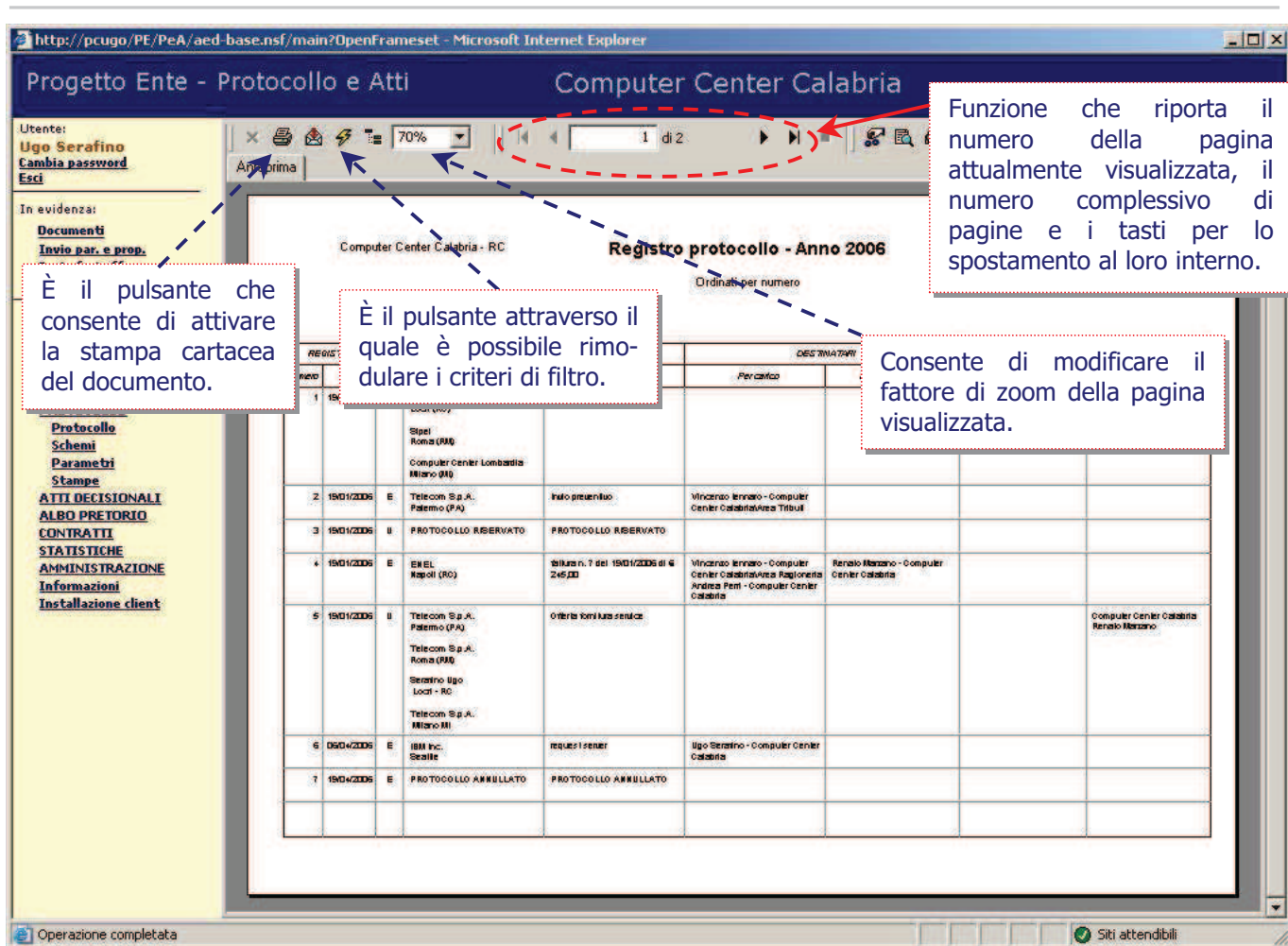


Figura 37 - Stampa Registro

La prima icona visibile sullo schermo (a forma di stampante) è quella che consente di stampare il documento su supporto cartaceo.

Una funzione particolarmente interessante (raffigurata sullo schermo dall'icona a forma di fulmine) è quello che consente di rimodulare i criteri con i quali sono stati filtrati i dati, attivando la quale verrà fornita all'utente la possibilità di operare all'interno dei criteri di filtro come visto precedentemente nelle Figura 32-36-37-38 senza dover ripetere tutta la procedura di stampa. I dati vengono aggiornati automaticamente.

La visualizzazione standard del foglio in anteprima è posta al 100% il che vuol dire che vengono riprodotte le dimensioni reali della pagina (solitamente A4) sul quale verranno stampati i dati. Per avere una visualizzazione di un'area maggiore o minore si può intervenire modificando a piacimento il fattore di zoom nell'apposito menu a tendina, queste variazioni non si percuoteranno sul risultato finale.

La funzione "Trova" (rappresentata dal binocolo) consente di cercare, all'interno del documento visualizzato, le parole chiavi inserite dall'operatore. La funzione è simile a quella

presente su tutti i principali editor di testo. Anche questa funzionalità è in linea con quanto disposto dall'art. **58 del D.P.R. 445/2000**.

*... “La ricerca delle informazioni del sistema è effettuata secondo criteri di selezione basati su tutti i tipi di informazioni registrate. I criteri di selezione possono essere costituiti da espressioni semplici o da combinazioni di espressioni legate tra loro per mezzo di operatori logici. Per le informazioni costituite da testi deve essere possibile la specificazione delle condizioni di ricerca sulle singole parole o parti di parole contenute nel testo”.*

Abbiamo visto in questo paragrafo tutte le fasi della procedura di stampa partendo dall'opzione “Stampa Registro Protocollo” (Figura 31). Andiamo ad analizzare le altre opzioni disponibili cioè:

- 1) Stampa Registro Protocollo per UO;
- 2) Stampa Registro Protocollo per Fascicolo;
- 3) Stampa distinta protocolli in uscita;
- 4) Stampa etichette.

2) **Stampa Registro Protocollo per UO**: ogni amministrazione comunale può disporre di più Unità Operative (UO), in questo caso il responsabile dell'ufficio può decidere di stampare i protocolli di competenza di una determinata UO. Per fare questo è sufficiente cliccare in corrispondenza dell'opzione “Stampa Registro Protocollo per UO” e successivamente selezionare l'UO desiderata. Così come per i seguenti altri punti (n. 3, 4 e 5) occorrerà completare con i dati richiesti e confermare con OK per ottenere i risultati voluti.

3) **Stampa Registro Protocollo per Fascicolo**: in questo caso i filtri saranno utilizzati sulla base dei procedimenti amministrativi attivati all'interno dell'Ente.

4) **Stampa distinta protocolli in uscita**: questa funzione permette di visualizzare la stampa distinta dei protocolli in uscita del registro e fornisce anche indicazione degli addebiti dei costi di spedizione per ciascun intestatario.

5) **Stampa etichette**: consente di stampare i dati dell'intestatario su un formato etichette 105x35 mm (due colonne da otto etichette su formato A4).

Abbiamo visto nelle pagine precedenti come sia possibile impostare differenti criteri per ottenere la stampa dei protocolli. La funzionalità che viene attivata dal pulsante indicato in Figura 38, consente

di esportare i dati del protocollo nei principali formati utilizzati sul mercato. Questa funzionalità consente di avere un archivio elettronico organizzato in files che possono essere utilizzati e condivisi da diversi applicativi. Inoltre, la loro conservazione e memorizzazione su supporti magnetici diventa più semplice da gestire dal momento che la lettura dei dati memorizzati non richiede necessariamente l'utilizzo dell'applicativo che le ha prodotte.

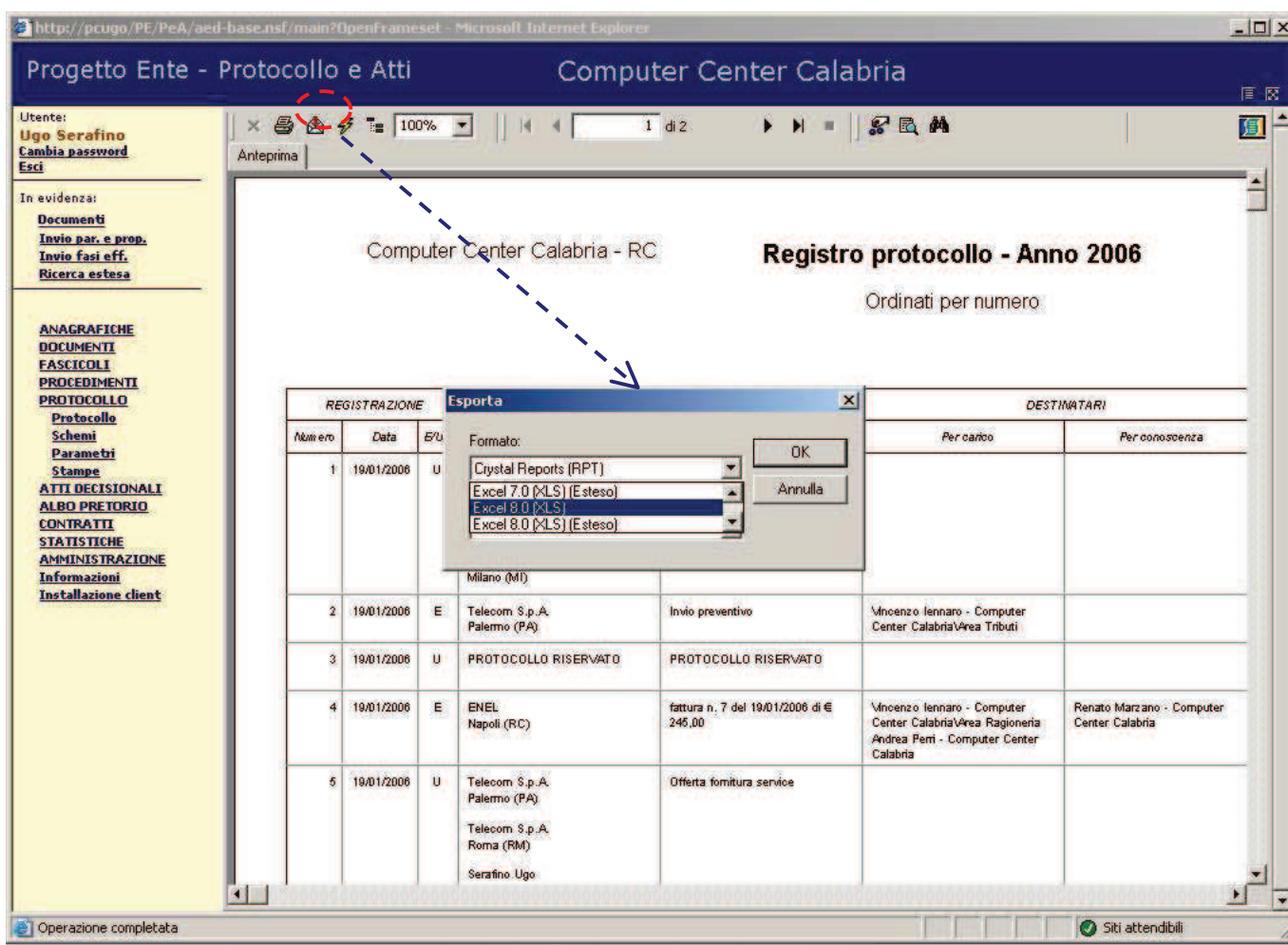


Figura 38 - Stampa Registro

## 6 FUNZIONALITÀ E UTENTI

Nel presente paragrafo facendo riferimento a quanto stabilito nell'art.7 del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 in merito alle garanzie di accesso alle informazioni agli utenti abilitati, verranno presentati alcuni esempi che riguarderanno le autorizzazioni e le funzionalità concesse a determinati utenti.

Il responsabile dell'Ufficio del protocollo è la risorsa all'interno dell'Ente a cui è affidato il compito di assegnare le abilitazioni sulle funzionalità del protocollo informatico.

Ad esempio stabilisce che all'interno dell'ufficio una determinata risorsa è abilitata alla funzione di "Gestore Protocollo" oppure "Gestore Ufficio Protocollo". Le modalità attraverso le quali il responsabile assegna le autorizzazioni prescinde dagli obiettivi del presente manuale e non verrà commentato. Nel seguito vedremo quali operazioni l'applicativo consentirà di utilizzare ad un utente generico a cui non è stata assegnata nessuna funzione rispetto a quello a cui è affidata la funzione di "Gestore Protocollo" e di "Gestore Ufficio Protocollo".

La ridotta visualizzazione delle schede non rappresenta la sola limitazione assegnata ad un utente non abilitato. Infatti se l'utente procede all'apertura della scheda "Protocollo" (vedi Figura 39) si troverà a non poter creare un protocollo perché il pulsante "Nuovo Protocollo" non è attivato. Può tuttavia aprire un protocollo e vedere le informazioni in esso contenute.

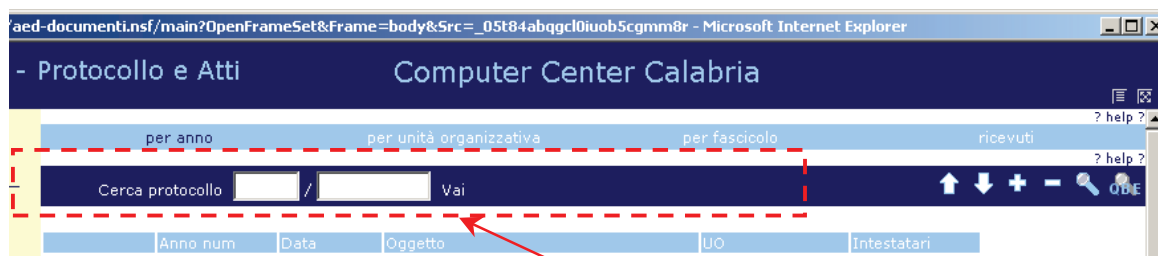


Figura 39 - Utente Generico

Per l'utente generico la funzione **Nuovo Protocollo** non risulta disponibile, tuttavia può aprire un protocollo in visualizzazione e può accedere alle funzioni di ricerca.

Anche in questo caso l'utente generico può semplicemente consultare i dati contenuti all'interno del protocollo senza poter apportare modifiche di nessun genere (Acquisisci Immagini, Crea Copia, ecc..) non essendo abilitato a visualizzare il pulsante di modifica.



PROTOCOLLO: Oggetto del documento con due mittenti

Modifica

? help ?

Vai a...

**DATI OBBLIGATORI**

Numero 101	Data protocollo 07/10/2008 15:31	Entrata/Uscita/Interno E *	Data
Mittente	Ragione sociale Albertini Stefano	Indirizzo Viale dei Trenta, 13 30020 Varese - VA	Vedi
Oggetto	Oggetto del documento con due mittenti		
Estremi doc orig	Data red doc	Nr all	

**DESTINATARI INTERNI** Organizzazione operativa

Documento collegato

UO COMUNE D'ITALIA\AFFARI GENERALI

Destinatario	Ruolo permesso	Responsabile Area Affari Generali	Traccia destinatari
--------------	----------------	-----------------------------------	---------------------

**DATI CLASSIFICATIVI**

Descrizione			
Antecedente		Sussequente	
Mezzo postale	- seleziona un mezzo -	Data postale	

Visualizza altri dati

L'unica funzione attiva è quella che consente all'utente di abbandonare la presente vista.

Figura 40 - Utente Generico

Oltre alla scheda "protocollo" l'utente generico è abilitato, limitatamente alle funzionalità del protocollo, a visualizzare gli "schemi" anche in questo caso senza essere autorizzato ad apportare alcuna modifica.

SCHEMA PROTOCOLLO: Comunicazione ai Capigruppo

? help ?

Vai a...

<b>Identificativo schema</b>	Schema protocollo *		
<b>Descrizione</b>	Comunicazione ai Capigruppo *		
<b>Entrata / Uscita / Interno</b>	U		
<b>Oggetto</b>	Invio comunicazioni Capigruppo		
	Destinatari:	Email	Tipo invio
	1 - primo	mpert tv.it	
	2 - secondo	mpé tv.it	
<b>Titolario d'archivio</b>	2/3/		
<b>Descrizione titolario</b>	Organi di governo, gestione, controllo, consulenza e garanzia / Consiglio		
<b>Materia \ Argomento</b>	comunicazioni		

Anche in questa vista la voce **Modifica** non sarà disponibile, avremo infatti esclusivamente il pulsante **di abbandono**

Figura 41 - Utente Generico

Come si può notare infatti nella Figura 41 l'unico pulsante attivo è quello che consente di chiudere la vista e di ritornare alla pagina iniziale del protocollo.

Il caso che verrà presentato di seguito riguarda, invece, un utente che è stato abilitato alla funzione di “Gestore di Protocollo”. Rispetto al caso precedente l’utente oltre ad essere abilitato a vedere le schede relative a “protocollo” e “schemi” può, all’interno di esse, effettuare tutte le operazioni previste dall’applicativo (come evidenziato in Figura 20).

L’utente “Gestore Ufficio Protocollo”, oltre alle funzionalità precedenti è abilitato a visualizzare “Parametri” e “Stampe” e ad operare all’interno di esse secondo tutte le modalità previste dall’applicativo.

## 7 FUNZIONE DI NAVIGAZIONE “VAI A ..”

La navigazione all’interno dell’applicativo è affidata alla funzione “Vai a..” presente, in ogni videata, nell’angolo in alto a destra.



Figura 42 – Funzione di navigazione

Tranne nel caso delle videate presentate in pop-up, dove l’abbandono può avvenire cliccando sulla funzione “Chiudi” o semplicemente chiudendo la videata stessa, in ogni altra situazione i comportamenti di abbandono da tenersi sono di seguito descritti.

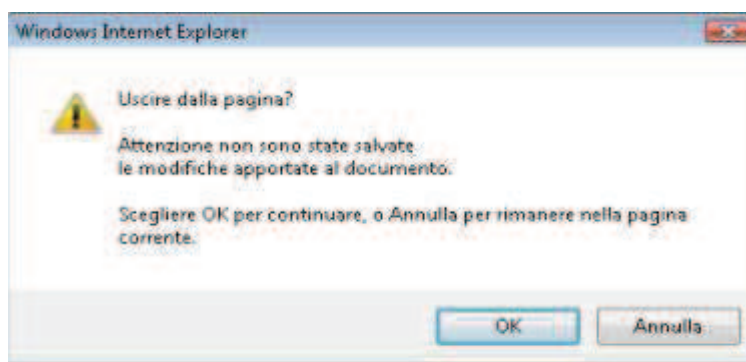
Posizionandosi con il mouse sulla voce **Vai a...** viene immediatamente presentato l’elenco delle ultime visualizzazioni fatte dall’utente ( con un limite posto a 10 visualizzazioni )



**Figura 43** – Elenco delle operazioni eseguite

L'utente potrà quindi cliccare su una qualsiasi delle scelte disponibili dall'elenco ottenendo come risultato l'abbandono della maschera nella quale è posizionato e la presentazione delle informazioni relative alla scelta effettuata.

Qualora l'operatore abbia inserito dati e, senza aver salvato le modifiche, cerchi di abbandonare la maschera di caricamento ( anche cliccando sulla "X" che chiude la sessione di lavoro ), otterrà dall'applicativo la seguente segnalazione



Che invita l'operatore o, premendo su "Ok" per abbandonare la maschera senza procedere alla memorizzazione delle operazioni effettuate ( ovvero rinunciando a salvare i dati caricati ), o, cliccando su "Annulla", ritornare sulla maschera di caricamento e da lì procedere con il salvataggio dei dati prima di abbandonare la maschera.

\*\*\*\*\* fine documentazione \*\*\*\*\*