Manuale di Gestione
del Protocollo Informatico

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce

Sommario

Sezione I
Ambito di applicazione

1.1. Introduzione

Le pubbliche amministrazioni, entro il 31 dicembre 2003, dovevano dotarsi di un protocollo informatico, secondo quanto stabilito dal pacchetto normativo della riforma Bassanini, in particolare dal DPR 20 ottobre 1998, n. 428, confluito per lo più nel DPR 28 dicembre 2000, n. 445, contenente il *Testo unico delle norme sulla documentazione amministrativa*.
L'art. 5 del DPCM 31 ottobre 2000, contenente le *Regole tecniche sul protocollo informatico*, prevede che le pubbliche amministrazioni redigano un *Manuale* per la gestione del protocollo, dei flussi documentali e degli archivi(, cioè il documento che qui si presenta).
Si tratta di uno strumento operativo che, per il grado di analisi che ogni amministrazione deve effettuare, può rappresentare da un lato il riconoscimento strategico del protocollo come sistema documentale integrato, dall'altro un primo e significativo passo verso la certificazione di qualità del servizio medesimo.
Il dettato del DPCM prevede che il *Manuale* affronti alcuni aspetti cruciali, quali la gestione e la tenuta dei documenti su vari supporti, la migrazione dei documenti informatici, l'introduzione dei titolari di classificazione e dei massimari di selezione dei documenti, oltre che la parte legata al "*recordkeeping system*" ed al "*workflow management*".
Il sistema di Protocollo Informatico è un sistema modulare che si compone di un nucleo base che assolve a funzionalità minime in quanto permette le operazioni di registratura, segnatura e classificazione che costituiscono funzioni necessarie e sufficienti per la sua tenuta. Il sistema è predisposto per essere integrato con funzionalità aggiuntive necessarie alla gestione dei flussi documentali, alla conservazione dei documenti ed all'accessibilità delle informazioni.
Il protocollo informatico è dunque uno snodo irrinunciabile del sistema informativo documentale, a condizione che siano garantiti l'interoperabilità, la trasparenza e il controllo dell'azione amministrativa attraverso i documenti che ogni Camera di Commercio produce nell'esercizio della propria attività pratica.
Questo manuale, descrive le fasi operative del sistema per la gestione del protocollo informatico, dei flussi documentali e degli archivi, individuando per ogni azione o processo i rispettivi livelli di esecuzione, responsabilità e controllo, dal protocollo all'archivio storico. Reso pubblico attraverso la pubblicazione sul sito internet www.le.camcom.it, esso potrà servire per il cittadino-cliente come primo livello di *Carta dei Servizi*.
Alla fine del *Manuale* si trova un breve glossario dei termini tecnici usati più frequentemente.

1.2 Azioni preliminari

1.2.1 Area Organizzativa Omogenea (AOO)

La Camera di Commercio di Lecce è un'Area Organizzativa Omogenea (AOO) in quanto insieme definito di Unità Organizzative (UO) che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali.

1.2.2 Descrizione del servizio Archivio: istituzione e funzioni

L'archivio della Camera di Commercio di Lecce è costituito dal complesso dei documenti prodotti e acquisiti dall'ente nello svolgimento della propria attività e nell'esercizio delle proprie funzioni. Esso comprende anche i fondi archivistici di enti ed istituti cessati, le cui funzioni e/o proprietà sono state trasferite alla Camera di Commercio.
L'Archivio è unico: le suddivisioni in archivio corrente, archivio di deposito e archivio storico sono solo gestionali.
Per quanto attiene all'archivio corrente, le modalità tecniche ed operative per la gestione di detto archivio sono le stesse indipendentemente dal luogo fisico ove è collocato.
L' accesso alla documentazione presente in archivio è regolata dalle norme vigenti in materia di accesso ai documenti amministrativi.

1.2.3 Individuazione del servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi

Nell'ambito della Camera di Commercio di Lecce è istituito un Servizio per la tenuta del protocollo Informatico, la Gestione Documentale e gli Archivi, ai sensi dell'art. 61 comma 1 DPR 445/2000.
Il servizio è posto all'interno dell'Area p.o. "Affari Generali" della Ripartizione I. Ad esso è preposto un funzionario in possesso di idonei requisiti professionali o professionalità tecnico-archivistica acquisite a seguito di percorsi formativi specifici, oltre al personale addetto, adeguato per numero e qualifica, in rapporto alle esigenze dell'Ufficio Protocollo-Archivio.

1.2.4 Introduzione del protocollo informatico ed eliminazione dei protocollo interni

Con l'entrata in vigore del protocollo informatico (01.01.2004) cessano di fatto e di diritto tutti i cosiddetti protocolli interni (cioè di settore, protocolli multipli, ecc.) e tutti gli altri sistemi di registrazione dei documenti diversi dal protocollo unico.
Rimangono tuttavia in vigore, sulla base di indicazioni normative o regolamentari, alcuni registri di protocollo particolare (v. paragrafo 2.5).
Il responsabile del servizio di protocollo, anche tramite il responsabile di A.p.o. e gli addetti, esegue periodicamente controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale, e sull'utilizzo di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie Unità Organizzative, la validità dei criteri di classificazione e fascicolazione utilizzati.

Sezione II
Le tipologie documentarie

2.1 Il documento amministrativo - definizioni

Per documento amministrativo viene inteso ogni rappresentazione grafica, fotografica, sonora, informatica o di qualsiasi altra specie del contenuto di atti o fatti giuridicamente rilevanti, anche interni, prodotti ed acquisiti ai fini dell'attività amministrativa, così come prevede l'art. 22 comma 2 della legge 7 agosto 1990, n° 241. e l'art. 1 del DPR 28 dicembre 2000, n° 445 e successive modifiche e integrazioni.

2.1.1. Il Documento informatico

Per documento informatico viene inteso qualsivoglia supporto informatico contenente dati o informazioni aventi efficacia giuridico-probatoria, cioè la rappresentazione informatica di atti , fatti o dati giuridicamente rilevanti, così come prevede l'art. 3 della legge 23 dicembre 1997, n° 547 e l'art. 1, c. 1, lett. B) del DPR 445/2000 e successive modifiche e integrazioni.

2.1.1.1 Versione analogica di un documento informatico

Per versione analogica di un documento informatico si intende una copia, di norma cartacea, di un documento amministrativo prodotto in origine su supporto informatico.

2.1.2 Il documento analogico

Per documento analogico viene inteso un documento amministrativo prodotto su supporto non informatico.
Di norma il documento analogico è un documento cartaceo prodotto con strumenti analogici (es. lettera scritta a mano o a macchina) o con strumenti informatici (es. lettera prodotta mediante un sistema di videoscrittura e stampata: come originale si considera quello cartaceo dotato di firma autografa ed eventualmente stampato su carta intestata): l'originale è analogico.

2.1.2.1 Versione informatica di un documento analogico

Per versione informatica di un documento analogico si intende una copia del documento amministrativo prodotta su supporto informatico (es. file risultante dalla scansione del documento cartaceo).

2.1.3 Registro

Per registro s'intende un documento amministrativo costituito dalla registrazione in sequenza, secondo criteri predefiniti (solitamente cronologici), in un'unica unità documentaria di una pluralità di atti giuridici.
In ambiente digitale i registri possono assumere la forma di database: sono detti "Sistemi informatici" e sono documenti informatici costituiti dall'insieme di una procedura informatica e di una base di dati gestite tramite dispositivi di elaborazione elettronica digitale (es. protocollo informatico).

2.1.4. Fascicolo

Per fascicolo si intende l'insieme dei documenti che afferiscono al medesimo procedimento amministrativo o che riguardano uno stesso affare o che appartengono ad una stessa tipologia.
Il fascicolo costituisce l'unità base, fondamentale per la gestione e la conservazione della documentazione relativa a ciascun procedimento o affare.
I documenti contenuti nel fascicolo sono ordinati cronologicamente in modo che l'atto più recente compaia per primo.

2.1.5 Serie

Per serie s'intende un raggruppamento, dettato da esigenze funzionali, di documenti con caratteristiche omogenee in relazione alla natura e alla forma dei documenti (serie delle determinazioni, dei contratti, dei registri di protocollo, …) o in relazione all'oggetto e alla materia (serie dei fascicoli personali, delle pratiche di finanziamento, …)

2.1.6 Firma digitale

Per firma digitale s'intende , a norma dell'art. 1 , c. 1, del DPR 445/2000 e successive modifiche e integrazioni, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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.
Le chiavi devono essere certificate con la procedura di cui all'art. 27 del DPR 445/2000 e successive modifiche e integrazioni. In particolare la certificazione di una chiave pubblica da parte di un'autorità di certificazione garantisce la corrispondenza della chiave con il soggetto che la espone.

2.1.7 Firma elettronica

Per firma elettronica s'intende, ai sensi dell'art. 2, c.1, lett. A) del D. Lgs. 10/2002, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite l'associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

2.1.8 Regime giuridico dei documenti della Camera di Commercio

A norma dell'art. 2, c. 1 lett. D) e c. 4, e dell'art. 55 del d. Lgs. 490/1999, tutti i documenti della Camera di Commercio di Lecce (analogici ed informatici, ricevuti, spediti o interni) dal momento del loro inserimento nell'archivio della Camera di Commercio mediante l'attribuzione di un codice di classificazione sono inalienabili.
In quanto beni culturali fin dall'origine, i singoli documenti e l'archivio nel suo complesso sono sottoposti a particolari tutele e garanzie: ai sensi degli artt. 21 e 22 del D. Lgs. 490/99 è necessario chiedere l'autorizzazione della Soprintendenza archivistica per lo spostamento dei fondi dell'archivio di deposito e dell'archivio storico, e per lo scarto di documentazione archivistica.
La Sovrintendenza archivistica ha poteri di vigilanza sull'archivio della Camera di Commercio di Lecce in quanto Ente Pubblico.
In attesa del riordino dell'archivio storico camerale, lo stesso è al momento parzialmente indisponibile ai fini dell'accesso da parte dell'utenza con particolare riferimento ai documenti che per la loro vetustà e stato di conservazione non possono essere maneggiati se non con rischio di danneggiamento o distruzione.

2.2 Le tipologie di documenti

I documenti si distinguono in documenti in arrivo, documenti in partenza e documenti interni.
I documenti ricevuti e spediti sono oggetto di registrazione di protocollo, ad esclusione dei documenti soggetti a registrazione particolare e dei documenti non soggetti a registrazione di protocollo.
I **documenti in arrivo** sono tutti i documenti pervenuti alla Camera di Commercio.
I documenti in partenza sono i documenti prodotti nell'esercizio delle proprie funzioni dal personale in servizio presso la Camera di Commercio e diretti all'esterno (destinatari esterni all'ente).
I **documenti interni** sono i documenti scambiati tra differenti UO della Camera di Commercio.

In base all'art. 53 c. 5 del DPR 445/2000, tutti i documenti ricevuti e spediti dalle amministrazioni sono oggetto di registrazione obbligatoria, ad eccezione di alcune tipologie particolari (cfr. 2.2.1) e dei documenti già sottoposti a registrazione particolare (cfr. 2.5).

2.2.1 Documenti non sottoposti a registrazione

I documenti per i quali la Camera di Commercio di Lecce non effettua la registrazione nel sistema di protocollo informatico sono:

- gazzette ufficiali
- bollettini ufficiali
- notiziari della pubblica amministrazione
- materiali statistici
- atti preparatori interni
- giornali
- riviste
- libri
- opuscoli e pubblicazioni varie
- depliant
- materiali pubblicitari
- inviti a manifestazioni che non attivano procedimenti amministrativi
- tutti i documenti già soggetti a registrazione particolare dall'amministrazione
- documenti di occasione avente carattere effimero (ringraziamenti, richieste di appuntamento con i dirigenti, congratulazioni varie, condoglianze, ecc.)
- modulistica del personale
- la posta elettronica non avente valore legale o giuridico a parere dell'Ufficio competente

2.2.2. Divieto di registrazione a fronte

Ogni numero di protocollo individua un unico documento, attribuendogli data e provenienza certa.
Ciascun documento, pertanto, dovrà recare un solo numero di protocollo.
Non può quindi essere utilizzato lo stesso numero di protocollo per registrare un documento in risposta ad un documento in arrivo, utilizzando la cosiddetta registrazione "a fronte" e ciò neppure se il documento in partenza viene protocollato nel medesimo giorno o nella medesima sessione di registrazione del documento in arrivo.

2.2.3 Documenti interni

Per documenti interni si intendono i documenti scambiati tra le diverse Unità Organizzative Responsabili (UOR) afferenti alla medesima Area Organizzativa Omogenea.
Essi si distinguono in:
a) documenti di preminente carattere informativo;

b) documenti di preminente carattere giuridico-probatorio.

Rientrano in questa tipologia di documenti anche la corrispondenza da e per i diversi organi Camerali (Consiglio, Giunta, Collegio dei Revisori, Nucleo di Valutazione, Commissioni e Comitati).
I documenti interni di preminente carattere informativo sono di norma memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra uffici, e di norma non vanno protocollati.
I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, e, come tali, devono essere protocollati secondo le disposizioni previste nelle sez. 3 e 4.

2.3 Procedure per la formazione e il flusso di documenti interni

E' abilitato alla registrazione dei documenti interni solamente l'Ufficio Archivio e Protocollo.

Per i documenti interni valgono le stesse regole descritte per i documenti in partenza.

2.3.1 Documenti in partenza

Procedure per la formazione e spedizione dei documenti in partenza

I documenti prodotti, indipendentemente dal supporto sul quale sono stati scritti, devono riportare, opportunamente evidenziate e se disponibili, le seguenti informazioni:

a) logo della Camera di Commercio e dicitura "Camera di Commercio di Lecce";
b) unità organizzativa responsabile con l'eventuale indicazione dell'area e del servizio di appartenenza;
c) indirizzo completo della Camera di Commercio (via, numero, c.a.p., città, provincia, stato);
d) numero di telefono della CCIAA o della UOR;
e) numero di telefax della CCIAA o della UOR;
f) indirizzo di posta elettronica (vedi paragrafo "Uso della Posta Elettronica");
g) data completa (luogo, giorno, mese, anno) ;
h) numero di protocollo;
i) numero degli allegati;
j) descrizione degli allegati;
k) numero di collegamento o di riferimento ad un eventuale precedente;
l) oggetto del documento;
m) sigla del responsabile della immissione dei dati o composizione del testo;
n) indicazione per esteso del RPA (responsabile del procedimento amministrativo) con relativa sigla e/o del dirigente e relativa firma autografa.

2.3.2 Redazione del documento in partenza: originale e minuta

Ogni documento cartaceo in partenza o interno va di norma redatto in due esemplari, cioè in originale e in minuta.
Per **originale** si intende il documento nella sua redazione definitiva, completo delle informazioni di cui al precedente paragrafo e di firma.
Per minuta si intende l'originale del documento conservato "agli atti", cioè nel fascicolo relativo all'affare o al procedimento amministrativo trattato.
Anche la minuta va corredata di firma autografa e dalla dicitura "minuta".

2.3.3 Spedizione del documento in partenza

L'originale del documento deve essere consegnato all'Ufficio Archivio e Protocollo completo di tutto l'occorrente per la spedizione (buste indirizzate, ricevute di ritorno già compilate, allegati, ecc.).
Le modalità di spedizione devono essere indicate esplicitamente dal RPA all'Ufficio Protocollo; sarà inoltre cura del RPA segnalare casi particolari e concordare la modalità di spedizione più adatta con l'Ufficio Protocollo. In assenza di indicazioni la trasmissione del documento avverrà per "Posta prioritaria". In caso di spedizione a mezzo fax, detta modalità di trasmissione va indicata sul documento con la dicitura "trasmesso a mezzo fax".

2.3.3.1 Spedizione plurima di documenti in partenza

È consentito attribuire un unico numero di protocollo a più documenti identici in partenza, nel caso di molteplici destinatari, acquisendo con mezzi informatici la lista dei destinatari che dovrà quindi comparire tra gli allegati del documento.
Su ogni copia devono essere riportati numero e data di protocollo. In tal caso la registrazione di protocollo riporterà nello spazio del corrispondente una dicitura generica (es. "diversi", "Aziende Agricole", etc.) o il primo nominativo. L'elenco dei destinatari deve essere consegnato unitamente all'originale e alla minuta all'uff. Protocollo, affinché venga acquisito otticamente. Esso dovrà, inoltre, essere conservato, a cura del RPA, nel fascicolo di appartenenza, allegato alla minuta.
Il personale dell'uff. Protocollo effettuerà le operazioni di affrancatura e compilerà le eventuali distinte di spedizione.
Il materiale così predisposto verrà consegnato alle Poste Italiane di norma lo stesso giorno di registrazione.

2.3.3.2 Orari dell'Ufficio Archivio e Protocollo.

I documenti in partenza devono essere consegnati all'uff. Archivio e Protocollo nei seguenti orari:

entro le ore 11,00.

I documenti in partenza consegnati all'uff. Protocollo entro tale ora, verranno registrati, di norma, nella medesima giornata lavorativa e spediti nello stesso giorno.

I documenti in partenza consegnati all'ufficio protocollo al di fuori di tale orario verranno registrati, di norma, nella giornata lavorativa successiva.

Spedizioni che rivestono carattere di particolare urgenza devono essere segnalate al Responsabile del Servizio di protocollo informatico o, in caso di assenza o impedimento, al Responsabile Apo e/o al Responsabile dell'Ufficio Protocollo.

Le spedizioni particolarmente numerose devono essere segnalate per tempo al responsabile dell'Ufficio di protocollo informatico e i documenti dovranno pervenire all'ufficio Protocollo con un congruo anticipo.

Altre UOR possono essere abilitate alla protocollazione in partenza, sulla base delle valutazioni del Responsabile del servizio di protocollo e del Segretario Generale.

2.3.4 Documenti in arrivo

L'originale del documento va di norma inviato al responsabile del procedimento amministrativo.

2.4 Modalità di trasmissione dei documenti all'interno e all'esterno della AOO

2.4.1 Telefax

L'attività di registrazione dei telefax va preceduta da un'attenta valutazione che discerna ciò che può e deve essere registrato da ciò che non deve essere registrato. L'uso del telefax soddisfa il requisito della forma scritta, e, quindi, non deve essere seguito dalla trasmissione del documento originale.

a) Il documento in arrivo deve essere protocollato insieme alla copertina di trasmissione, se presente. La segnatura di protocollo deve essere effettuata sul documento e non sulla copertina.
Qualora il documento inviato via fax venga successivamente inviato anche per via ordinaria, dovrà essere rispettata la seguente procedura:
   1) Assicuratisi che trattasi del medesimo documento pervenuto via fax, si effettua la segnatura di protocollo riportando sul documento tutte le informazioni relative alla registrazione di protocollo già effettuata;
   2) Qualora il documento inviato per via ordinaria contenga elementi di diversità rispetto a quello inviato via fax (ad es., riporta numero e data di protocollo, precedentemente assenti) o non sia possibile accertarsi dell'identittà fra i due documenti, esso dovrà essere registrato con un nuovo numero di protocollo;
   3) In entrambi i casi, il documento inviato per via ordinaria dovrà essere conservato nel fascicolo di appartenenza, tenendo in allegato il documento inviato via fax.

b) Il documento in partenza deve essere protocollato prima della partenza, assieme alla copertina di trasmissione, se presente. Numero e data di protocollo devono essere apposti sul documento e non sulla copertina. Il documento deve riportare la dicitura "documento trasmesso a mezzo fax".

2.4.2 Uso della posta elettronica

Anche l'attività di registrazione della posta elettronica va preceduta da un'attenta valutazione sui documenti da registrare.
Ai sensi dell'art. 14 del DPR 445/2000 e s.m.i., nonché del D. Lgs. 7.3.2005 n. 82 (codice dell'amministrazione digitale) aggiornato dal D. Lgs. N. 159 del 4.4.2006 (Disposizioni integrative e correttive al d. Lgs. 7.3.2005 n. 82) un documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

In particolare:

1) "I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
2) Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Pertanto La Camera di Commercio di Lecce ha definito la casella di posta elettronica certificata istituzionale cciaa@le.legalmail.camcom.it e ne ha chiesto l'iscrizione presso l'IPA (Indice delle Pubbliche Amministrazioni), gestito dal Centro Tecnico della R.U.P.A.

Qualora i messaggi di posta elettronica pervengano alla casella di posta elettronica certificata istituzionale e posseggano i requisiti indicati dal CNIPA, essi vengono registrati nel sistema di protocollo informatico della Camera di Commercio.

Gli Uffici e dipendenti camerali, titolari di caselle di posta elettronica, in caso di ricezione di messaggi di posta elettronica certificata da parte di soggetti esterni, sono tenuti, indicando la presenza di informazioni o dati di interesse per l'Amministrazione, a inoltrare tali messaggi all'Ufficio protocollo per la protocollazione in arrivo.
L'implementazione di caselle di posta elettronica certificata oltre alla casella di posta elettronica certificata istituzionale è valutata e decisa dal responsabile del protocollo sentiti i dirigenti interessati.

Qualora il documento inviato per posta elettronica certificata venga successivamente inviato anche per via ordinaria, viene rispettata la seguente procedura:

a) l'operatore di protocollo si assicura che si tratti del medesimo documento pervenuto per posta elettronica certificata ed effettua la segnatura del documento riportando tutte le informazioni relative alla registrazione di protocollo già effettuata;
b) qualora il documento inviato per via ordinaria contenga elementi di diversità rispetto a quello inviato per posta elettronica (ad es., riporta numero e data di protocollo, precedentemente assenti) o non sia possibile accertarsi dell'identità fra i due documenti, esso viene registrato con un nuovo numero di protocollo;

c) in entrambi i casi, il documento inviato per via ordinaria deve essere conservato nel fascicolo di appartenenza, tenendo in allegato il documento inviato via posta elettronica.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dall'AIPA, e si renda necessario attribuire un'efficacia probatoria al documento ricevuto, dovrà essere rispettata la seguente procedura:
. il documento in arrivo deve essere di norma stampato con l'apposizione della dicitura "documento ricevuto via posta elettronica" ed è successivamente acquisito per via ordinaria a cura del responsabile del procedimento amministrativo.

2.5 Tipologie particolari di documenti per i quali si stabiliscono modalità di protocollazione particolare

Si riportano di seguito le tipologie di documenti per le quali la Camera di Commercio di Lecce prevede modalità di registrazione particolare e pertanto non vanno registrati nel sistema di protocollo informatico.

2.5.1 Delibere e determinazioni

Le delibere e le determinazioni in quanto documenti già soggetti a registrazione particolare da parte dell'Amministrazione, di norma non vanno registrati nel protocollo generale.

2.5.1.1 Serie delle Delibere e delle Determinazioni e rispettivo repertorio generale

Ciascun complesso delle delibere e delle determinazioni costituisce una serie.
Ciascuna serie delle delibere e delle determinazioni deve essere corredata da un proprio repertorio generale.
Nel repertorio generale va riportato un numero progressivo, denominato "numero di repertorio", che identifica il documento all'interno della serie.
Il repertorio generale ha cadenza annuale, cioè inizia il 1° gennaio e termina il 31 dicembre di ogni anno.
Sono istituiti i seguenti repertori:
a) delibere di Giunta
b) delibere di Consiglio
c) determinazioni e atti del Presidente
d) determinazioni dirigenziali del Segretario Generale e dei Dirigenti

L'istituzione di nuovi repertori è disposta dal Segretario Generale.

Presso gli uffici Affari Generali sono conservati i repertori generali e le serie relativi agli ultimi cinque anni. I repertori generali e le serie esaurite da oltre cinque anni vanno versati all'archivio di deposito.

2.5.1.2 Gestione e archiviazione delle delibere e delle determinazioni

Per ogni delibera e determinazione devono essere prodotti di norma due esemplari (un originale e una minuta), ferme restando le copie dichiarate conformi e le copie di carattere informativo riprodotte per le esigenze d'ufficio.
L'originale va conservato nella rispettiva serie (serie delle delibere, serie delle determinazioni) e ordinato secondo il numero di repertorio; la minuta, invece, va conservata nel rispettivo fascicolo (e/o sottofascicolo, inserto), cioè insieme ai documenti che afferiscono al medesimo procedimento.

2.5.2 Registro delle Denunce al Registro delle Imprese

Le seguenti tipologie di documento:
a) le domande di iscrizione, modifica o cancellazione dal R.I e dal R.E.A., sia quelle presentate allo sportello che quelle inviate per posta senza lettera di accompagnamento
b) le domande di vidimazione dei libri contabili

sono soggette a registrazione particolare da parte dell'Ufficio del Registro Imprese.
Tutte le altre tipologie di documento, quali, ad es.:
a) le richieste di accertamento inviate a coloro che hanno presentato le domande
b) l'invio dei suddetti accertamenti da parte dei diretti interessati
c) le richieste di visure/certificati/elenchi inviate per posta
d) l'invio di visure/certificati/elenchi

non sono soggette a registrazione particolare da parte dell'Ufficio del Registro Imprese , e vengono registrate nel protocollo informatico dell'Ente.

2.5.3 Registro dei Protesti Cambiari

Le seguenti tipologie di documento:
a) l'elenco Protesti consegnato dall'Ufficiale Levatore,
b) le istanze di cancellazione consegnate dal protestato
c) le istanze di annotazione consegnate dall'Ufficiale Levatore.

sono soggette a registrazione particolare da parte dell'Ufficio Protesti.
Tutte le altre tipologie di documento, quali, ad es.:
a) le comunicazioni di reiezione
b) le richieste di rettifica pervenute da parte dell'Ufficiale Levatore
c) le comunicazioni prevenute dai Tribunali

non sono soggette a registrazione particolare da parte dell'Ufficio Protesti, e vengono registrate nel protocollo informatico della CCIAA di Lecce.

2.5.4 Registro delle Domande di Brevetti e Marchi

Le seguenti tipologie di documento:
a) domande di registrazione marchi;
b) domande di rilascio brevetti ;
c) Invio telematico domande brevetti al Ministero competente

sono soggette a registrazione particolare da parte dell'Ufficio Marchi e Brevetti,. Tutte le altre tipologie di documento,non sono soggette a registrazione particolare da parte dell'Ufficio Brevettri, e vengono registrate nel protocollo informatico dell'Ente.

2.5.5 Registro dei Verbali di Sanzione(ex-Upica)

I verbali di accertamento e di sequestro, le ordinanze di ingiunzione, le ordinanze di confisca o dissequestro sono soggette anche a registrazione particolare da parte dell'Ufficio ex Upica. Tutte le altre tipologie di documento, quali, ad es.:

a) l'invio di memorie difensive o controdeduzioni
b) l'invio di notifiche e prescrizioni

non sono soggette a registrazione particolare da parte dell'Ufficio ex Upica, e vengono registrate nel protocollo informatico dell'Ente.

2.5.6 Registro dei M.U.D.

I modelli di dichiarazione ambientale (Mud) sono soggette a registrazione particolare da parte dell'Ufficio Ambiente.
Tutte le altre tipologie di documento, non sono soggette a registrazione particolare da parte dell'Ufficio Ambiente , e vengono registrate nel protocollo informatico dell'Ente.

2.5.7 Registro delle Denunce ad Albi, Ruoli, Elenchi e Licenze

Le seguenti tipologie di documento:

a) tutte le domande di iscrizione, modifica o cancellazione dagli albi, ruoli ed elenchi tenuti dalla Camera di Commercio
b) tutte le richieste di licenza inviate alla Camera di Commercio

sono soggette a registrazione particolare da parte degli Uffici competenti.
Tutte le altre tipologie di documento, quali, ad es.:

a) le richieste di accertamento dei titoli e dei requisiti morali inviate alle Questure, Prefetture e ai Tribunali.;
b) le comunicazioni in uscita,
c) Le D.I.A. (Dichiarazioni d'inizio attività) per le attività di cui alla L. n. 46/90 e n. 122/92)

non sono soggette a registrazione particolare da parte degli Uffici competenti, e vengono registrate nel protocollo informatico dell'Ente.

2.5.8 Registro delle Fatture

Le fatture attive emesse sono soggette a registrazione particolare da parte dell'Ufficio Ragioneria.
Tutte le altre tipologie di documento, quali, ad es.:

a) le fatture passive ricevute dall'Ente
b) le ricevute dei bollettini di pagamento

non sono soggette a registrazione particolare da parte dell'Ufficio Ragioneria, e vengono registrate nel protocollo informatico dell'Ente.

2.5.9 Registro dei certificati di origine

Le richieste di certificati di origine sono soggette a registrazione particolare da parte dell'Ufficio Commercio Estero.

2.5.10 Registro dei Verbali di Seduta

Le seguenti tipologie di documento:

a) verbali della Giunta Camerale
b) verbali del Consiglio Camerale

sono soggette a registrazione particolare da parte dell'Ufficio Affari Generali e pertanto non vengono registrati nel protocollo informatico dell'Ente.

2.5.11 Ordini di Servizio

Gli Ordini di servizio sono soggetti a registrazione particolare da parte dell'Ufficio Personale, pertanto, non vengono registrati nel sistema di protocollo informatico della Camera di Commercio.

2.5.12 Registri carte tachigrafiche

Le carte tachigrafiche, trasmesse dal gestore del sistema informatico direttamente all'Ufficio Metrico, vengono consegnate agli utenti finali direttamente dagli addetti dell'Ufficio stesso, previe operazioni di registrazione previste dal sistema informatico effettuate dagli stessi addetti.

Tutte le altre tipologie di documenti:

a) domande di emissione di carte tachigrafiche
b) domande di emissione di carta del conducente
c) richieste di verifiche metriche e/o di rilegalizzazione di strumenti metrici
d) comunicazioni di utilizzo di strumenti metrici

vengono registrate nel protocollo informatico generale dell'ente.

2.6 Individuazione dei supporti utilizzati

Viene autorizzata la riproduzione informatica dei documenti, sia in arrivo che in partenza, a fini esclusivamente gestionali, e non con finalità sostitutive dell'originale. In attesa di nuove e specifiche direttive dettate dall'Autorità per l'informatica nella pubblica amministrazione, nonché dell'emanazione di standard internazionali per la conservazione dei documenti su supporto non cartaceo che non pregiudichino la certezza del diritto e l'efficacia probatoria, è differito pertanto l'utilizzo delle tecnologie informatiche e dei supporti informatici per finalità di conservazione.

Sezione III
La descrizione dei flussi documentali

3.1 Procedure per la ricezione dei documenti in arrivo (acquisizione, smistamento, assegnazione)

Posta in arrivo

La corrispondenza indirizzata alla sede di V.le Gallipoli, 39 della CCIAA di Lecce viene consegnata dal servizio Pick-up delle Poste Italiane di norma alle ore 10,30.
Il personale addetto all'ufficio protocollo provvede all'apertura di tutta la posta tranne quella di cui al punto 3.1.1..
La posta consegnata all'ufficio Metrico di P.zza Mazzini di Lecce viene recapitata di norma quotidianamente all'ufficio protocollo.
La posta consegnata alla sede decentrata di Casarano viene recapitata alla sede centrale di Lecce – ufficio protocollo a mezzo corriere camerale normalmente n. 1 volta la settimana.
La corrispondenza consegnata brevi manu ai vari uffici deve essere tempestivamente consegnata all'ufficio protocollo.

3.1.1 Documenti in arrivo da non aprire

La corrispondenza non viene aperta nei seguenti casi:

a) corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara;
b) corrispondenza indirizzata nominativamente (senza indicazione dell'ente) oppure riportante l'indicazione "riservata", "personale", "confidenziale" o simili, o comunque dalla cui confezione si evinca il carattere di corrispondenza privata.

La corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili o comunque dalla cui confezione si evinca la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo e della data di registrazione direttamente sulla busta (plico o simili).
Aperta la busta (plico o simili), il responsabile del procedimento amministrativo provvede a riportare il numero di protocollo e la data di registrazione già assegnati al documento, conservando la busta (plico o simili) come allegato.

3.1.2. Casi particolari.:

a) lettere anonime
Nel caso di lettere anonime queste non sono registrate al protocollo, ma formalmente inoltrate, se contengono informazioni o dati di interesse per l'Amministrazione, agli uffici di competenza i quali valutano l'opportunità se dare seguito a queste comunicazioni ed individuano le eventuali procedure da sviluppare.
Le mail indirizzate da postazioni di posta elettronica non certificata all' indirizzo PEC della CCIAA Lecce (messaggi del cittadino) sono assimilate alle lettere anonime.

b) Lettere prive di firma
Le lettere prive di firma vanno protocollate. Sarà poi compito della UOR e, in particolare, del RPA valutare caso per caso, ai fini della loro efficacia riguardo ad un affare o un determinato procedimento amministrativo, se la lettera priva di firma è da ritenersi valida.

c) Documenti di competenza di altre amministrazioni

Qualora pervenga alla Camera di Commercio un documento di competenza di altro Ente, altra persona fisica o giuridica, lo stesso viene trasmesso a chi di competenza, se individuabile, viceversa viene restituito al mittente.
Nel caso in cui un documento non di competenza della CCIAA di Lecce venga erroneamente protocollato, esso verrà spedito a chi di competenza accompagnato da una lettera di trasmissione opportunamente protocollata. L'ufficio protocollo provvederà altresì ad annullare il protocollo del documento erroneamente acquisito.

d) Originali plurimi (ad esempio comunicazioni identiche indirizzate a più destinatari interni all'ente e riportanti lo stesso numero di protocollo) che pervengono in tempi successivi: viene protocollato solo il primo esemplare pervenuto che viene trasmesso a tutti i destinatari presenti sul documento. Gli altri originali non sono protocollati ma vengono consegnati direttamente al destinatario. In ogni caso gli addetti dell'ufficio protocollo annoteranno sul documento data ed estremi della registrazione.

e) Documenti privi di allegati.
Gli addetti dell'ufficio protocollo rileveranno, con apposita annotazione sull'atto, la mancanza di allegati di cui invece è fatta menzione nel testo del documento.

3.1.3 Timbro di arrivo

Prima della registrazione viene apposto su ogni documento il timbro d'arrivo (timbro tondo con scritta Camera di Commercio Industria Artigianato e Agricoltura di Lecce e data)
Il timbro di arrivo viene apposto, per la corrispondenza in arrivo, direttamente sul documento, dopo l'apertura.
Fa eccezione la corrispondenza che riporta esplicitamente la dicitura gara, concorso o simili, per la quale il timbro di arrivo viene apposto sulla busta o confezione.

3.1.4 Registrazione di un documento in arrivo

La registrazione dei documenti in arrivo è di esclusiva competenza dell'Ufficio Protocollo.

a) La registrazione del documento in arrivo avviene attraverso la registrazione, nel sistema di protocollo informatico "Prodigi" degli elementi riportati nel paragrafo 4.2

3.1.5. Segnatura dei documenti in arrivo

La segnatura di protocollo è l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso. Viene effettuata, dal personale addetto alla registrazione del documento, contestualmente alla registrazione stessa.
Essa consiste nell'apposizione, sul documento in arrivo, del timbro di protocollo riportante le seguenti informazioni:

a- nome identificativo dell'amministrazione (Camera di Commercio Industria Artigianato e Agricoltura – Lecce);
b- la data di protocollo;
c- il numero di protocollo, costituito da sette cifre numeriche; tale numerazione si rinnova ad ogni inizio di anno solare;
d- indice di classificazione del documento.

Solo per la corrispondenza riportante la dicitura gara, concorso o simili, la segnatura di protocollo sarà apposta sulla busta o plico.
Sarà poi cura del RPA riportare sul documento le informazioni della segnatura di protocollo, conservando la busta o plico come allegato al documento.

3.1.6 Smistamento e assegnazione dei documenti in arrivo

I documenti, dopo la registrazione, classificazione, segnatura vengono smistati ai Dirigenti di Ripartizione in cartelle intestate alle diverse UOR., sulla base delle competenze di cui all'unito organigramma camerale., e da questi siglati e trasmessi ai responsabili delle UOR. In caso di assenza del dirigente i documenti saranno trasmessi al Responsabile di area e dopo la sigla ai responsabili delle UOR.
Chiunque si accorga di aver ricevuto tra la propria corrispondenza un documento inerente procedimenti di competenza di altra unità organizzativa responsabile , deve consegnarlo o farlo pervenire tempestivamente all' ufficio protocollo che aggiornerà l'ufficio assegnatario.
Qualora venga erroneamente registrato un documento di competenza di terzi (altro ente, altra persona fisica o giuridica), la registrazione va annullata utilizzando un altro numero di protocollo per la trasmissione a chi di competenza.
Le comunicazioni interne da protocollare devono essere limitate allo stretto indispensabile. Fatta salva la possibilità di effettuare comunicazioni interne, tramite protocollo, nel rispetto del rapporto gerarchico :

- ✓ dovrà essere sviluppata la comunicazione informale anche via e-mail tra uffici diversi ;
- ✓ le comunicazioni interne tra uffici appartenenti ad aree di posizione diverse (A.P.O.) devono essere vistate dal Dirigente di Ripartizione o dal Segretario Generale in caso di assenza o impedimento del Dirigente ;
- ✓ le comunicazioni tra uffici diversi della stessa area p.o. devono essere vistate dal Responsabile A.P.O. o dal Dirigente in caso di assenza o impedimento del Responsabile A.P.O.;
- ✓ le comunicazioni interne tra uffici di Ripartizioni diverse devono essere a firma del Dirigente della Ripartizione o vistate dallo stesso e indirizzate al Dirigente della Ripartizione di destinazione.

L'assenza dei prescritti visti ricade sotto la personale responsabilità del mittente. Nessun controllo, in merito, deve essere effettuato dall'ufficio protocollo.

3.1.7 Documenti afferenti a più affari o procedimenti amministrativi

Qualora un documento tratti più argomenti, imputabili a procedimenti amministrativi o affari diversi, è possibile farne il necessario numero di copie.

3.1.8 Protocollo differito

Qualora dalla mancata registrazione a protocollo del documento nel medesimo giorno lavorativo di ricezione possa venire meno un diritto di terzi, con motivato provvedimento del responsabile del servizio di protocollo si differiscono i termini di registrazione a protocollo.
Per differimento dei termini di registrazione si intende il provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione a protocollo deve comunque essere effettuata.
Su ciascun documento ammesso al differimento della registrazione, dovrà comunque essere apposto il timbro d'arrivo.
Per evitare ritardi e garantire una più efficiente gestione delle procedure relative allo svolgimento di gare, concorsi e simili, gli uffici della Camera di Commercio dovranno comunicare all'Ufficio Protocollo e Archivio, con congruo anticipo, l'indizione di gare, concorsi e simili.

3.1.9 Rilascio di ricevute

Qualora un documento sia consegnato personalmente dal mittente o da altra persona incaricata e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'ufficio protocollo fotoriprodurrà gratuitamente la prima pagina del documento ricevuto e vi apporrà il timbro di arrivo e la propria sigla.
Dal giorno lavorativo successivo a quello di rilascio della ricevuta sarà possibile rivolgersi all'ufficio protocollo per ottenere l'indicazione del numero di protocollo assegnato al documento.

Sezione IV
La registrazione dei documenti nell'applicazione "Prodigi"

Il sistema di Protocollo Informatico è un sistema modulare che si compone di un nucleo base che assolve a *funzionalità minime* in quanto permette, come previsto dalla normativa in vigore, le operazioni di *registratura*, le operazioni di *segnatura* nonché le operazioni di *classificazione* che costituiscono funzioni necessarie e sufficienti per la sua tenuta.

4.1 **Elementi del protocollo**

Il protocollo è composto da elementi obbligatori e da elementi gestionali.

La registrazione degli elementi obbligatori del protocollo è rilevante sul piano giuridico-probatorio mentre la registrazione degli elementi gestionali del protocollo è rilevante sul piano organizzativo-gestionale.

4.1.1 Gli elementi obbligatori del protocollo (Registratura)

Gli elementi obbligatori del protocollo, cioè quelli rilevanti sul piano giuridico-probatorio, sono:

a) il numero di protocollo generato automaticamente dal sistema e registrato in forma "non modificabile", costituito da 7 cifre;
b) la data di registrazione assegnata automaticamente dal sistema e registrato in forma "non modificabile", sarà espressa nel formato giorno/mese/anno con l'anno composto di quattro cifre;
c) il mittente per i documenti ricevuti o il destinatario per i documenti spediti;
d) l'oggetto;
e) data e numero di protocollo del documento ricevuto qualora siano disponibili;
f) l'impronta del documento informatico qualora sia stato inviato per via telematica;
g) l'indice di classificazione.

4.1.2 Registrazione cosiddetta "a fronte"

Ogni numero di protocollo individua un unico documento, attribuendogli data e provenienza certa. Ciascun documento, pertanto, recherà un solo numero di protocollo.
Non può quindi essere utilizzato lo stesso numero di protocollo per registrare un documento in risposta ad un documento in arrivo utilizzando la cosiddetta registrazione "a fronte", neppure se questa viene effettuata nel medesimo giorno o nella medesima sessione di registrazione del documento in arrivo.

4.2 Gli elementi gestionali del protocollo

Nel protocollo informatico vengono registrati elementi gestionali il cui scopo è di rendere quanto più efficace ed efficiente l'azione amministrativa; questi elementi assumono rilevanza solo sul piano organizzativo e gestionale. Sono suddivisi sulla base delle funzionalità cui afferiscono in:

a) dati di registrazione:
    1. data di arrivo (nel formato giorno/mese/anno con l'anno composto di quattro cifre);
    2. tipo di spedizione (posta ordinaria, corriere espresso, raccomandata con ricevuta di ritorno, telefax, ecc.);
    3. il numero degli allegati, compresi inserti e annessi;
    4. descrizione degli allegati;

b) dati per il controllo dei procedimenti amministrativi:
    1. unità organizzativa responsabile del procedimento amministrativo (UOR);

c) per la gestione dell'archivio:
    1. classificazione del documento attraverso il titolario (categoria, classe e fascicolo).

4.3 Annullamento di una registrazione di protocollo

Il Responsabile dell'Ufficio Protocollo o gli addetti, qualora necessario, effettuano l'annullamento delle registrazioni, previo avviso al Responsabile del Protocollo Informatico e al Responsabile dell'Area "Affari Generali".
L'operazione avviene attraverso l'apposizione nel sistema della dicitura «annullato».
Per indicare l'annullamento la procedura riporta una dicitura ed un segno in posizione sempre visibile e tale, comunque, da consentire in tutti i casi la lettura di tutte le informazioni precedentemente registrate.

4.4 Inalterabilità, immodificabilità e validità degli elementi obbligatori

Nell'ipotesi in cui si dovesse ricorrere alla modifica anche di una sola delle informazioni generate o assegnate in maniera automatica dal sistema, bisogna annullare l'intera registrazione come descritto nel paragrafo precedente.
Nel caso di eventuale annullamento anche di una sola delle altre informazioni registrate in forma non modificabile, il sistema, contestualmente all'aggiornamento del dato con i valori corretti, memorizza nella banca dati il contenuto precedente assieme alle informazioni relative alla data, l'ora ed all'autore della modifica.

4.5 Registri

4.5.1 Registro di protocollo

E' un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento/spedizione del documento, indipendentemente della regolarità del documento stesso.
Esso è idoneo a produrre effetti giuridici a favore o a danno delle parti, e pertanto, è soggetto alle forme di pubblicità e tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

4.5.2 Registro giornaliero

Il *Registro giornaliero* di protocollo è costituito da tutte le informazioni inserite nell'arco dello stesso giorno con le funzioni di registrazione.

4.5.3 Registro di emergenza

Il responsabile del servizio per la tenuta del protocollo informatico autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su registri di emer-

genza, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora d'inizio dell'interruzione nonché la data e l'ora di ripristino della funzionalità del sistema. Le unità di personale autorizzate alla registrazione dei documenti su registri di emergenza sono le unità appartenenti all'Area Affari Generali abilitate alla protocollazione.
Il responsabile dell'Ufficio Protocollo tiene i registri di emergenza, su cui effettua le necessarie annotazioni, previo avviso al Responsabile del Protocollo Informatico e al Responsabile dell' Area Affari Generali.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattr'ore, per cause di eccezionale gravità, il responsabile del servizio 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.
Per ogni giornata di registrazione manuale è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. La sequenza numerica utilizzata sul registro di emergenza costituisce una sequenza autonoma e riparte dal n. 1 per ogni anno di utilizzo. La sequenza numerica anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico, dal numero successivo all'ultimo registrato prima dell'interruzione.
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.

Sezione V
Organizzazione e gestione dell'archivio corrente (classificazione e fascicolazione)

5.1 Tenuta del sistema di classificazione: procedure di mantenimento e aggiornamento

5.1.1. Titolario di classificazione

Per titolario di classificazione si intende un quadro alfanumerico di riferimento per l'archiviazione, la conservazione e la individuazione dei documenti.
Il titolario di classificazione si suddivide in categorie, le quali si suddividono in classi e sottoclassi.
Ogni classe o sottoclasse ha un numero variabile di fascicoli, in relazione agli affari e ai procedimenti amministrativi trattati. Essi vengono numerati progressivamente all'interno della classe o sottoclasse di appartenenza e annotati nel repertorio dei fascicoli.

5.1.2 Aggiornamento del titolario

Il titolario di classificazione delle Camere di Commercio è stato elaborato da un apposito gruppo di lavoro costituito all'interno del Comitato Tecnico Scientifico degli Archivi delle Camere di Commercio che suggerisce alle camere gli aggiornamenti periodici.
La Camera di Commercio di Lecce ha adottato il titolario con deliberazione n. 4 del 16.1.2001. La Camera di Commercio può apportare integrazioni al suddetto titolario su indicazione del Responsabile del Protocollo Informatico e degli Archivi.
Il titolario di classificazione adottato è contenuto in allegato al presente manuale.

5.2 Il fascicolo: individuazione, gestione e tenuta

Il fascicolo è individuato da tre elementi:
a) l'anno di apertura (o di *istruzione*);
b) l'indice di classificazione
c) l'oggetto, cioè una stringa di testo per descrivere compiutamente un affare o un procedimento amministrativo o più di questi insieme.

5.3 Definizione degli strumenti di reperimento (mezzi di corredo)

Gli strumenti per descrivere un archivio (o un fondo o una serie o comunque delle unità archivistiche), a seconda del grado di analisi e dello scopo per il quale vengono approntati, possono essere un inventario, repertorio, elenco di consistenza, elenco di versamento, indice, rubrica, ecc.

Tutti gli strumenti di corredo sopracitati devono necessariamente seguire le stesse regole che hanno portato alla definizione della struttura e dei campi del titolario di classificazione.
Lo strumento di reperimento più importante è il repertorio dei fascicoli, cioè l'elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe o sottoclasse e riportante tutti i dati del fascicolo.
Attualmente la Camera di Commercio di Lecce non dispone di alcuno di questi strumenti di gestione dell'archivio.

Sezione VI
Organizzazione e gestione dei documenti semi-attivi (archivio di deposito)

6.1 Versamento dei fascicoli

Periodicamente - di norma una volta all'anno - e secondo un apposito piano di versamento stabilito dal massimario di selezione, ogni ufficio deve conferire al responsabile dell'Ufficio protocollo informatico i fascicoli relativi ad affari e a procedimenti amministrativi conclusi o comunque non piú necessari ad una trattazione corrente.
Ricevuti i fascicoli, il responsabile del protocollo informatico, con l'ausilio dei competenti addetti, predispone un elenco di consistenza e dispone il trasferimento del materiale nell'archivio di deposito.
I fascicoli *personali* vanno versati dall'archivio corrente all'archivio di deposito l'anno successivo alla data di cessazione dal servizio del dipendente.
Le serie e i repertori delle delibere e delle determinazioni, relative agli ultimi 5 anni sono, di norma, conservati presso l'Ufficio Affari Generali; trascorso tale termine, le serie e i repertori vengono, di norma, conferiti al responsabile del protocollo informatico per il versamento all'archivio di deposito.

6.2 Definizione delle responsabilità delle unità organizzative

Il responsabile del procedimento amministrativo è tenuto a conferire al responsabile del protocollo informatico i fascicoli relativi ad affari e a procedimenti amministrativi conclusi o comunque non più necessari ad una trattazione corrente, secondo la periodicità indicata nella sezione 6.1.

Sezione VII
Selezione dei documenti

La selezione è l'operazione con la quale vengono individuate le unità archivistiche da destinare alla conservazione permanente o da avviare allo scarto.
Il Segretario Generale, con apposito provvedimento, può istituire una commissione preposta ad effettuare la selezione di cui sopra.
Tale commissione deve predisporre un elenco di documenti di cui proporre lo scarto.
Tale elenco deve essere approvato dal Segretario Generale, e successivamente deve essere inviato alla Soprintendenza archivistica per l'autorizzazione.
Una volta ricevuta l'autorizzazione, i documenti possono essere distrutti.
La selezione deve comunque essere effettuata prima del passaggio dei fascicoli alla sezione separata dell'archivio storico.
Per effettuare la selezione si utilizza il massimario di conservazione o scarto adottato con deliberazione n. 358 del 19.12.2003.

Sezione VIII
Conservazione dei documenti informatici

Si è in attesa di sviluppare ulteriormente, insieme ad Infocamere, gli aspetti relativi alla conservazione dei documenti informatici .

Sezione IX
Piano per la sicurezza relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici

9.1 Analisi dei rischi

Un'accurata analisi dei rischi ai quali è esposta la Camera di Commercio richiede uno specifico intervento *ad hoc* che va oltre i confini di un Manuale di gestione. Per tale ragione in questo capitolo ci si limita a fornire una sintesi delle minacce più comuni ai sistemi informatici ed a evidenziare le funzioni di sicurezza ritenute necessarie, con particolare riguardo agli aspetti tecnologici. La seguente tabella evidenzia le relazioni tra minacce e funzioni di sicurezza.

Minacce \ **Funzioni di sicurezza**		Identif. e Autenticazio-	Controllo Accessi	Tracciabilità	Controlli Periodici	Riutilizzo Risorse	Accuratezza	Affidabilità del Servizio	Trasmissione Dati
M1	Introduzione di sw dannoso	**X**	**X**	**X**	**X**		**X**		
M2	Mal funzionamento sw (di sistema ed appl.)			**X**	**X**		**X**		
M3	Mal funzionamento hw			**X**	**X**		**X**		
M4	Mal funzionamento rete			**X**	**X**		**X**		
M5	Errore in fase di back-up			**X**	**X**				
M6	Errore in fase di aggiornamento, manutenzione del sw			**X**	**X**				
M7	Errore in fase di aggiornamento, manutenzione della rete			**X**	**X**				
M8	Sovrascrittura di memoria		**X**						
M9	Accesso non autorizzato al sistema	**X**	**X**	**X**	**X**				
M10	Acquisizione illecita di sw								
M11	Sovraccarico elaborativo del sistema	**X**	**X**	**X**	**X**			**X**	
M12	Sovraccarico delle linee di connessione			**X**	**X**			**X**	
M13	Intercettazione del traffico di rete			**X**	**X**				**X**
M14	Manipolazione di sw	**X**	**X**	**X**	**X**		**X**		
M15	Utilizzo illecito del sistema hw/sw	**X**	**X**	**X**	**X**				
M16	Alterazione instradamento rete	**X**	**X**	**X**	**X**				

Funzioni di sicurezza / Minacce		Identif. e Autenticazio-	Controllo Accessi	Tracciabilità	Controlli Periodici	Riutilizzo Risorse	Accuratezza	Affidabilità del Servizio	Trasmissione Dati
M17	Modifica privilegi di accesso	**X**	**X**	**X**	**X**				
M18	Mascheramento dell'identità utente	**X**	**X**	**X**	**X**				
M19	Acquisizione dati su supporti magnetici					**X**			
M20	Abuso di privilegi	**X**	**X**	**X**	**X**				
M21	Non rispetto della legislazione vigente	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Si osservi, per inciso, che alcune delle minacce ai sistemi informatici possono essere contrastate solo attraverso misure organizzative o logistiche.

9.2 Politiche di sicurezza

Le politiche di sicurezza sono la pietra angolare per garantire l'efficacia della sicurezza. Senza una politica sulla quale basare standard e procedure, è probabile che le decisioni siano inconsistenti e che ci siano "buchi" nella sicurezza, che possono essere sfruttati sia da persone interne sia da persone esterne all'organizzazione.
Nel seguito sono identificate le politiche di sicurezza adottate dalla Camera di Commercio.

9.2.1 Identificazione e Autenticazione (IA)

Il sistema deve sempre riconoscere e verificare l'identità di chiunque voglia accedere alle sue risorse.

9.2.2 Controllo degli Accessi (CA)

Il sistema deve garantire che gli utenti e i processi attivati dagli utenti non possano svolgere operazioni sulle informazioni o sulle risorse cui essi non sono autorizzati o di cui non hanno necessità.

9.2.3 Tracciabilità (TR)

Il sistema deve garantire la registrazione delle informazioni relative agli eventi causati da utenti o processi, in modo che le conseguenze di tali eventi possano essere, in seguito, associate all'utente in questione e gli si possa, pertanto, imputare la relativa responsabilità.

9.2.4 Controlli Periodici (CP)

Il sistema deve essere dotato di funzionalità per la registrazione di informazioni sugli eventi, tanto quelli di routine quanto quelli eccezionali, in modo che una indagine successiva possa determinare se si sono verificate violazioni della sicurezza e, in caso affermativo, quali informazioni o altre risorse sono state compromesse.

9.2.5 Riutilizzo Risorse (RR)

Il sistema deve essere dotato di funzionalità per garantire che le risorse (memoria centrale, aree di memoria su disco, etc) possano essere riutilizzate, senza pregiudicare la sicurezza.

9.2.6 Accuratezza (AC)

Il sistema deve essere dotato di funzionalità per garantire che siano correttamente preservate le relazioni specifiche tra diversi insiemi di dati e che i dati siano trasmessi da un processo all'altro senza subire alcuna alterazione. Inoltre il sistema deve essere dotato di funzionalità intese a identificare, segnalare e correggere violazioni all'integrità del software.

9.2.7 Affidabilità del Servizio (AS)

Il sistema deve essere dotato di funzionalità tali da garantire che l'accesso alle risorse sia possibile nel momento in cui risulta necessario

9.2.8 Trasmissione Dati (TD)

Il sistema deve essere dotato di funzionalità tali da garantire la sicurezza dei dati durante la loro trasmissione sui canali di comunicazione.

9.3 Interventi operativi

9.3.1 Per i documenti informatici formati dalle applicazioni di InfoCamere

Per i documenti informatici formati conseguentemente all'utilizzo di applicazioni InfoCamere si rinvia a quanto descritto nei manuali utente dei vari sistemi applicativi; in essi sono descritti gli accorgimenti adottati per salvaguardare l'integrità e la validità dei documenti informatici. Questa documentazione tecnica si trova nel sito Intranet appositamente predisposto dalla società stessa, costantemente aggiornato.

9.3.2 Per i documenti informatici formati dalle applicazioni proprie dell'ente.

Per la sicurezza dei documenti informatici, formati dalle applicazioni di produttività individuale (Word, Excel, ecc.) e/o da applicazioni proprie dell'ente vengono suggeriti alcuni interventi operativi che devono essere verificati, validati e complementati da parte della Camera. Tali interventi sono una modalità di attuazione delle politiche precedentemente descritte.
La sigla con cui è identificato ciascun interento suggerito corrisponde alla sigla di una delle politiche precedentemente descritte.

IA.1 Il sistema deve impedire l'accesso all'utente se il tentativo di accesso avviene al di fuori dei tempi di validità delle credenziali dell'utente.

IA.2 Il sistema deve rifiutare l'impostazione di credenziali al di fuori degli standard stabiliti (per esempio in caso di password essa deve rispettare requisiti del tipo: lunghezza minima e massima, tipi di caratteri utilizzabili, dizionario dei termini non utilizzabili).

IA.3 Deve essere garantita la segretezza dei valori di autenticazione, a tal scopo:
- non devono essere mostrati sul video quando digitati
- non devono essere incluse o registrate in nessun modulo o applicazione cui danno accesso.

IA.4 Il sistema deve essere provvisto di funzioni che garantiscano l'accesso alle informazioni di identificazione e autenticazione a chi autorizzato e ne impediscano l'accesso a chi non autorizzato.

IA.5 Il numero di tentativi di identificazione/autenticazione deve essere limitato ad un massimo.

IA.6 Il sistema non deve indicare, in caso di errore, il motivo che lo ha provocato.

IA.7 Deve essere possibile impostare limite minimo e limite massimo del tempo necessario ad effettuare le operazioni di identificazione e autenticazione.

CA.1 Per ogni tentativo di accesso ad un oggetto il sistema deve verificare la validità della richiesta.

CA.2 Il sistema deve mostrare un messaggio di *warning* quando avviene un tentativo di accesso non autorizzato.

CA.3 Tentativi di accesso non autorizzato devono essere respinti, registrati e quindi evidenziati.

CA.4 Deve essere limitata la deduzione di informazioni, tramite aggregazione di dati a cui si ha accesso legittimo.

CA.5 Deve essere garantito che:
- vengano individuati e bloccati flussi di informazioni illeciti,
- vengano assicurati flussi di informazioni leciti.

CA.6 I diritti di accesso devono avere valore limitato nel tempo.

CA.7 Non deve essere possibile, per chiunque non sia un utente autorizzato, di accedere alle liste di accesso.

CA.8 I diritti di accesso devono essere gestiti a livello centrale al fine di limitarne la propagazione incontrollata.

CA.9 Il sistema deve garantire che un utente possa effettuare le operazioni che è autorizzato ad intraprendere (p.es. lettura, modifica, esecuzione, presa di possesso), inoltre deve impedire che l'utente possa effettuare operazioni per le quali non è autorizzato.

CA.10 Il sistema deve permettere di impostare i diritti di accesso per gruppi di utenti; inoltre deve permettere di impostare i diritti per singoli utenti nel caso di risorse, applicazioni e dati particolarmente critici.

CA.11 Occorre predisporre funzionalità che impediscano l'apertura di un numero di sessioni superiore a quello prefissato.

CA.12 Deve essere possibile fissare un periodo di tempo che deve trascorrere tra l'ultima azione dell'utente e la chiusura automatica della sessione.

CA.13 Dopo la connessione il sistema deve mostrare l'ultimo log con esito positivo ed eventualmente quello con esito negativo.

TR.1 Il sistema deve consentire di scegliere le informazioni da registrare, ossia deve essere in grado di registrare e archiviare gli eventi definiti come rilevanti per la sicurezza.

TR.2 L'attività di registrazione deve essere sempre attiva.

TR.3 Deve essere possibile registrare selettivamente le azioni di uno o più utenti.

TR.4 I dati registrati devono essere resi disponibili ai soli addetti all'amministrazione della sicurezza. Non deve essere permesso agli utenti non autorizzati di accedere alle informazioni registrate.

TR.5 La registrazione deve essere effettuata mediante l'utilizzo di dispositivi di registrazione affidabili.

TR.6 Le informazioni registrate devono essere conservate per un periodo di tempo commisurato alla normativa vigente.

TR.7 Devono esistere ed essere documentati gli strumenti per esaminare e mantenere i file di tracciamento.

TR.8 Gli strumenti di analisi devono permettere di evidenziare selettivamente le attività di uno o più utenti.

CP.1 Il sistema deve consentire di scegliere le informazioni da registrare, ossia deve essere in grado di registrare e archiviare gli eventi e le relative informazioni specificati.

CP.2 L'attività di registrazione deve essere sempre attiva.

CP.3 Gli strumenti di audit, le segnalazioni ed i risultati delle analisi devono essere accessibili solo agli addetti all'amministrazione della sicurezza e agli addetti alle attività di auditing.

CP.4 La registrazione deve essere effettuata mediante l'utilizzo di dispositivi di registrazione affidabili.

CP.5 Le informazioni registrate devono essere conservate per un periodo di tempo commisurato alla normativa vigente

CP.6 Il sistema deve essere in grado di evidenziare, tra tutti gli eventi registrati, quelli che rientrano nella tipologia (predefinita) di eventi anomali o sospetti.

CP.7 Il sistema deve essere in grado evidenziare on-line gli eventi che rientrano nella tipologia per la quale è stata stabilita tale necessità e impostare le stazioni di lavoro su cui tali eventi devono essere evidenziati.

CP.8 Le revisioni sui file di log deve essere effettuata periodicamente.

CP.9 Gli strumenti di analisi devono essere disponibili e documentati.

CP.10 Gli strumenti di analisi devono permettere di eseguire almeno le operazioni di ricerca, selezione e ordinamento dei dati di audit in base a criteri logici definiti.

CP.11 Gli strumenti di analisi devono consentire di identificare selettivamente le azioni eseguite da uno o più utenti.

CP.12 Devono essere previsti strumenti per l'analisi di tendenza, finalizzata all'individuazione di eventuali violazioni dei requisiti di sicurezza, ancor prima che si producano.

CP.13 Devono essere previsti strumenti per la verifica dell'efficienza delle misure di sicurezza tecnologiche installate.

CP.14 Devono essere previste verifiche periodiche che mirano alla verifica della attuazione e della consistenza delle procedure utilizzate.

RR.1 Il sistema deve essere dotato di funzionalità che provvedano ad una adeguata inizializzazione degli oggetti di supporto ai dati.

RR.2 Devono essere previste funzionalità che, al termine delle operazioni, rendano non più utilizzabili i dati contenuti nelle aree di disco destinate a file temporanei, spool o log.

RR.3 Il riutilizzo dei supporti magnetici rimovibili (nastri magnetici, dischetti) deve essere preceduto dalla cancellazione dei dati in essi contenuti; tale cancellazione deve essere effettuata in modo tale da rendere impossibile la ricostruzione dei dati.

RR.4 I terminali devono essere dotati di screen saver con password, tali che:

- lo screen saver si avvii automaticamente dopo un intervallo di tempo stabilito dall'ultimo comando digitato dall'utente,
- la password abbia le stesse caratteristiche definite per l'Identificazione e Autenticazione.

RR.5 La sessione di lavoro si deve sospendere automaticamente dopo un determinato intervallo di tempo in cui l'operatore non ha inviato comandi al sistema.

AT.1 Il sistema deve essere dotato di funzioni intese a stabilire e mantenere la correttezza delle relazioni tra i dati, ad esempio funzioni che analizzano l'integrità degli indici di una base dati.

AT.2 Il sistema deve essere dotato di funzioni intese a rilevare e prevenire la compromissione (perdita, aggiunta o alterazione) dei dati quando scambiati tra utenti, processi ed oggetti.

AT.3 Il sistema deve essere dotato di funzioni atte a rilevare ed impedire che vengano modificate la fonte e/o destinazione del trasferimento dei dati.

AT.4 Il sistema deve essere dotato di funzionalità che consentano:

- l'identificazione e l'eliminazione di software dannoso (p.es. virus),
- la verifica dell'integrità degli eseguibili,
- la verifica della correttezza delle chiamate ai dati.

AT.5 Le funzionalità di controllo del software devono essere sempre attive.

AS.1 Deve essere garantita l'accessibilità e l'utilizzabilità delle risorse da parte di un'entità (processo o utente) autorizzata.

AS.2 Occorre limitare e/o prevenire le interferenze in operazioni cui il tempo riveste importanza cruciale.

AS.3 Il sistema deve essere dotato di funzioni di individuazione dell'errore.

AS.4 Il sistema deve essere dotato di funzioni atte a ridurre l'impatto degli errori.

AS.5 Il sistema deve essere dotato di funzioni atte a ridurre al minimo ogni eventuale arresto e o interruzione del sistema.

AS.6 Il sistema deve essere dotato di funzioni di schedulazione che garantiscono che il sistema risponda agli eventi esterni e produca risultati nei tempi previsti.

TD.1 Devono essere cifrate le eventuali password in caso di identificazione e autenticazione remota.

TD.2 I dati che fluiscono nella rete devono essere protetti mediante l'utilizzo di algoritmi crittografici, in funzione della Sensibilità dei Dati.

TD.3 Nel caso di necessità di cifratura dei dati, essi devono essere cifrati prima di essere immessi nella rete.

TD.4 Devono essere previste funzionalità atte al controllo degli accessi ai servizi di rete.

TD.5 Devono essere previste funzionalità di non-ripudio del mittente: quando un soggetto riceve informazioni in uno scambio di dati, tali funzionalità evidenziano sempre il mittente delle informazioni, in modo tale che quest'ultimo non possa in seguito negare di avere inviato tali informazioni.

TD.6 Devono essere previste funzionalità di non-ripudio del destinatario: quando un soggetto invia informazioni in uno scambio di dati, tali funzionalità evidenziano sempre il destinatario delle informazioni, in modo tale che quest'ultimo non possa in seguito negare di avere ricevuto tali informazioni.

TD.7 Devono essere previste funzioni di rilevazione di:

- errori sui dati trasmessi,
- manipolazioni non autorizzate dei dati di un utente e dei dati di tracciamento
- replica non autorizzata dei dati.

9.4 Suggerimenti comportamentali

In questa sezione viene fornita una panoramica sulle responsabilità spettanti a coloro che gestiscono documenti informatici e contemporaneamente vengono forniti dei suggerimenti comportamentali per l'utilizzo quotidiano degli strumenti informatici. Sicurezza intesa come riservatezza (autorizzazione all'accesso) ed integrità (protezione da incidenti o abusi).

9.4.1 Prevenire i virus.

I virus sono delle funzioni in grado di trasmettersi ed alimentarsi in maniera autonoma e possono causare effetti dannosi. Lo scopo della maggioranza dei virus è quello di intaccare le risorse dei computer presso i quali riescono ad installarsi arrivando, in molti casi, a distruggere tutto il contenuto delle memorie del sistema.
I virus si trasmettono attraverso programmi provenienti da fonti non ufficiali o attraverso l'utilizzo delle istruzioni macro previste nei programmi per l'automazione d'ufficio.
I momenti topici nei quali maggiore è il rischio di trasmissione di queste funzioni infettanti sono:

- quando si installano dei programmi,
- quando si copiano dati da floppy disk,
- quando si scaricano dati da Internet.

Per prevenire il propagarsi dei virus è importante che vengano utilizzati solo programmi provenienti da fonti fidate, bisogna assicurarsi che la fase di avvio del proprio computer non venga fatta partendo da un dischetto e, soprattutto, verificare periodicamente il livello di aggiornamento del software antivirus installato.

9.4.2 Gestione delle password.

Il sistema più semplice per accedere ai sistemi è quello di individuare la password che ne protegge l'intrusione; una password "complicata" è un elemento importante nel sistema di sicurezza informatica dei dati e dei documenti e le migliori password sono quelle facili da ricordare ma che contemporaneamente sono difficili da indovinare.
Di seguito alcune cose da fare o da non fare per meglio utilizzare le potenzialità dell'utilizzo delle password:

- Non si devono comunicare ad altri non solo le proprie password ma neanche i criteri utilizzati per costruirle e ricordarle.
- Non si deve scrivere la password su un giallino attaccato al monitor del computer o all'interno del cassetto della scrivania, sono luoghi ovvi e chiunque avrebbe l'opportunità di appropriarsene.
- Non si devono usare parole legate alla persona (nome, cognome, date di nascita, figli, numero di telefono, ecc.).
- Si deve cambiare periodicamente la password; la stessa che deve avere dimensioni abbastanza significative in relazione al fatto che la difficoltà aumenta in maniera esponenziale con l'aumentare del numero dei caratteri usati.
- Per quanto non espressamente indicato nel presente manuale in materia si fa riferimento al documento programmatico di sicurezza (DPS) della camera di commercio di Lecce.

La persona cui fare riferimento per ogni consiglio in merito è il responsabile dei sistemi operativi .

9.4.3 Ulteriori accorgimenti.

9.4.3.1 Utilizzo delle chiavi.

Un ulteriore importante accorgimento per rendere sicuri i dati ed i documenti in proprio possesso è il costante utilizzo delle chiavi dei mobiletti e delle porte dove vengono riposti i sistemi e le banche dati.
Una porta chiusa non impedisce definitivamente l'intrusione nei locali da parte di estranei, ma costituisce certamente un primo ostacolo il cui superamento è il prodotto di un atto volontario. Aprire una porta per danneggiare quanto disponibile sulla scrivania o per carpire informazioni facilmente reperibili è fin troppo facile.

9.4.3.2 Supporti per backup e stampe.

I supporti nei quali vengono ricoverati i dati di salvataggio delle informazioni riservate possono essere magnetici (floppy disk) o tradizionali (output su stampante); in entrambi i casi si deve avere cura di metterli in cassetti chiusi a chiave non appena finito di usarli e, nel caso della stampante, è opportuno ritirare quanto prima i documenti prodotti.

9.4.3.3 Gestione delle password.

Nell'utilizzo dei sistemi informatici ci sono più livelli di password:

- chiesta dal sistema operativo nella fase di avvio del computer,
- quando si intende accedere alla rete (sia Intranet che Internet),

- la password prevista dai sistemi specifici per la produzione,
- quella chiesta dal salvaschermo per i momenti in cui si lascia incustodita la postazione di lavoro.

Si devono utilizzare tutti questi livelli di password avendo cura di mantenerle distinte tra loro. Nell'ipotesi di doverne comunicare una qualsiasi ad un terzo soggetto, bisogna aver cura di cambiarla quanto prima possibile. Quando si digitano e soprattutto quando si cambiano le password bisogna aver cura di non farsi vedere (come quando si usa il bancomat).

Sezione X
Sicurezza del sistema Protocollo Informatico

10.1 Definizione dei diritti di accesso e profili utente

10.1.1. Responsabile del protocollo informatico

Il responsabile del protocollo è il Dirigente della Ripartizione I, salvo espressa delega ad altro funzionario di categoria D. La delega può investire parte delle proprie competenze.
Egli, anche tramite gli operatori del protocollo, può, per esempio:

predisporre le autorizzazioni di accesso al sistema;
eseguire la stampa del registro di protocollo giornaliero;
monitorare le operazione compiute.

Il responsabile del protocollo informatico ha accesso, anche tramite, gli operatori del protocollo, a tutti i dati del protocollo stesso.
Il responsabile del protocollo esegue controlli a campione sulla congruenza fra il titolario di classificazione e gli strumenti di corredo dell'archivio.
In caso di assenza o impedimento del responsabile del protocollo e degli eventuali delegati, le relative funzioni sono assicurate dal Segretario Generale o da chi ne fa le veci.

10.1.2 Operatore di Protocollo

L'operatore di protocollo è la persona che ha l'autorizzazione ad eseguire la registrazione dei documenti in arrivo e/o partenza e/o interni. Egli può acquisire (a seconda dei diritti e del profilo con cui è registrata la sua utenza nel sistema) l'immagine del documento mediante uno scanner, oppure associare il file prodotto da un programma informatico per la composizione di testi o per l'elaborazione di fogli elettronici, o per disegno tecnico o altro (es.: Word, Excel, PowerPoint, AutoCad, ecc.).
A tutti i documenti protocollati in arrivo, partenza e interni, l'operatore di protocollo attribuisce la classificazione (categoria e classe).

10.1.3 Responsabile del procedimento RPA

È l'assegnatario dei documenti ed è abilitato all'apertura e alla chiusura dei fascicoli ed all'inserimento dei documenti nei fascicoli stessi.
Ha la responsabilità della gestione del procedimento amministrativo per l'intero periodo di vita dello stesso e della verifica del corretto avanzamento delle varie fasi del procedimento con attenzione anche ai tempi di esaurimento delle singole fasi (qualora siano previsti).

10.1.4 Utente abilitato alla consultazione

L'utente consultatore è abilitato ad accedere al protocollo informatico limitatamente ai documenti ad esso assegnati o ai documenti degli uffici e dei servizi di propria competenza.

10.2 Regole per la tenuta del registro di protocollo di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico per effettuare le registrazioni di protocollo, ogni evento deve essere registrato su uno o più supporti alternativi (Registri di Emergenza). Su questi registri devono essere riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

Nell'ipotesi in cui l'impossibilità di utilizzare la procedura informatica si dovesse protrarre per un periodo superiore alle ventiquattro ore, deve essere rilasciata, da parte del responsabile di protocollo, specifica autorizzazione per l'uso del Registro di Emergenza. Il periodo massimo di autorizzazione all'utilizzo del registro di emergenza è pari ad una settimana ed in ogni caso devono essere riportati gli estremi del provvedimento di autorizzazione nel registro stesso.

Per ogni giornata in cui viene usato il registro di emergenza, è riportato sul registro stesso il numero totale di operazioni registrate .
La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico, dal numero successivo all'ultimo registrato prima dell'interruzione.

Le informazioni relative ai documenti protocollati con il registro di emergenza sono inserite nel protocollo informatico, utilizzando l'apposita funzione di recupero dei dati che verrà eseguita senza ritardo al ripristino delle funzionalità del sistema. Nel protocollo informatico saranno riportati tutti i dati trascritti nel registro di emergenza: ad ogni protocollo del registro sarà attribuito un nuovo numero di protocollo, secondo la numerazione del protocollo informatico, ed a questo sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

Sezione XI
Interoperabilità : descrizione livelli di attivazione delle funzioni di interoperabilità

Il sistema informatico di gestione protocollo “Prodigi” permette l’interoperabilità tra la Camera di Commercio, le altre amministrazioni e l’utente cittadino (cfr. 2.4.2).

Sezione XII
Accesso e protezione dei dati

Consultabilità dei documenti e protezione dei dati personali.

12.1 Organizzazione

E' individuata una sola Area Organizzativa Omogenea (A.O.O.) denominata Camera di Commercio Industria Artigianato e Agricoltura di Lecce, composta da tutte le sue strutture.
La Camera di Commercio è costituita da Unità Organizzative (UO): Ripartizioni o aree dirigenziali, servizi e uffici collocati anche in posizione di staff.

12.2 Visibilità dei protocolli

Con visibilità si intende, non solo la possibilità di vedere le proprietà del documento, ma anche il suo contenuto.

- I protocolli devono essere visibili dalla user che li ha inseriti e dalle user con pari abilitazioni (cioè tutte quelle dello stesso ufficio protocollo).
- Nel caso in cui una user sia abilitata alla sola protocollazione in uscita, essa deve avere visibilità solo sui protocolli da essa inseriti e non sui protocolli inseriti dalle altre user con pari abilitazione; tantomeno essa può vedere i protocolli inseriti dalle user con protocollazione generale.
- La visibilità dei protocolli deve essere piramidale: ogni UO può vedere i protocolli di tutto il settore (quindi i propri e quelli dei propri servizi, uffici, addetti); ogni servizio può vedere i protocolli di tutto il servizio (quindi i propri e quelli dei propri uffici, addetti); il capoufficio può vedere i protocolli propri e quelli dei propri addetti; ogni addetto può vedere solo i propri.
- Se una UO ha sotto di sé servizi o uffici o persone che rispondono gerarchicamente ad un'altra UO, la prima può vedere i protocolli dei servizi e/o uffici e/o persone che rispondono ad essa funzionalmente.
- Se un servizio ha sotto di sé uffici che rispondono gerarchicamente ad un altro servizio, il primo può vedere i protocolli degli uffici che dipendono funzionalmente da esso.
- Se un addetto svolge funzioni per uffici diversi, quando entra nel protocollo deve decidere per quale ufficio si presenta al sistema.
- E' inoltre possibile una gestione 'orizzontale' della visibilità: addetti che appartengono allo stesso UO/Servizio/Ufficio (compreso il Capo UO/Servizio/Ufficio) hanno la stessa visibilità; questa abilitazione è gestita a livello di singolo addetto.

12.3 Riservatezza dei protocolli

Le comunicazioni di carattere politico (es. comunicazioni tra Segretario Generale e membri di Giunta o Consiglio), la corrispondenza con Polizia/Carabinieri, i documenti personali e altre tipologie di documentazione riservata devono avere visibilità limitata in quanto "riservati".

L'addetto al protocollo decide, in base al tipo di documento o a quanto segnalato dal mittente, se trattasi di documento riservato. Per la posta in uscita la "riservatezza" del protocollo è stabilita dall'ufficio emittente.
In questo caso la consultazione è permessa solo al diretto assegnatario e non vale la gestione piramidale del protocollo. Quindi se il documento riservato è indirizzato ad un addetto, solo

quest’ultimo potrà consultarlo: né il suo diretto capoufficio, né il caposervizio, né il dirigente potranno consultarlo se non sono direttamente citati tra gli assegnatari.

L’oggetto inserito per questi protocolli dovrà essere generico.
L’amministratore del sistema, individuato nel responsabile dell’Ufficio, non può accedere a queste informazioni se non abilitato specificatamente. Per l'amministratore dovranno pertanto essere previste due abilitazioni distinte: una per la visibilità del sistema ed una per i documenti riservati.

12.4 Modifica dei protocolli

Se la protocollazione è centralizzata, l'Ufficio protocollo accede a tutti i protocolli per le modifiche; se la protocollazione avviene per singoli uffici, è possibile modificare soltanto il proprio protocollo.
Ogni operazione di modifica, che prevede la memorizzazione nel file di log dei codici identificativi dell'operatore, è possibile solo se l'operatore ne ha l'abilitazione.

Sezione XIII
Disposizioni finali

13.1 Modalità di adozione iniziale e degli aggiornamenti al manuale

Il Responsabile del Protocollo Informatico propone al Segretario Generale della Camera di Commercio l'adozione del Manuale di Gestione.
Il Segretario Generale adotterà un provvedimento finalizzato all'adozione del Manuale di Gestione.

13.2 Modalità di comunicazione del manuale

Il provvedimento adottato dal Segretario Generale della Camera di Commercio adempie all'obbligo di *comunicazione* del Manuale stesso mediante la pubblicazione all'Albo della Camera di Commercio.

13.3 Modalità di aggiornamento del manuale

Periodicamente il Responsabile del Protocollo Informatico propone aggiornamenti al Manuale di Gestione. Gli aggiornamenti possono riguardare anche solo una sezione o allegato del Manuale.
Gli aggiornamenti sono necessariamente previsti nei seguenti casi:

1. revisione del Titolario di classificazione;
2. revisione del Massimario di selezione;
3. variazioni sostanziali alle procedure informatiche;
4. modificazione degli assetti organizzativi della Camera di Commercio e cambiamenti dei procedimenti amministrativi;

13.4 Entrata in vigore

Il Manuale di gestione entra in vigore dal 23 maggio 2007

13.5 Ulteriori riferimenti

Per quanto non espressamente previsto dal presente manuale, si fa riferimento al documento programmatico di sicurezza (DPS) della camera di commercio di Lecce e alla normativa vigente in materia, adottando comportamenti ispirati al principio del buon andamento dell'attività amministrativa.

13.6 Istituzione della commissione per l'aggiornamento, la pubblicazione e l'applicazione del "Manuale di Gestione"

La Camera di Commercio di Lecce, con apposito provvedimento dirigenziale, può istituire una commissione, denominata "Commissione per l'aggiornamento, la pubblicazione e l'applicazione del Manuale di Gestione", con l'incarico di esaminare le problematiche inerenti al Protocollo Informatico e di Gestione Documentale.

13.6.1 Composizione della Commissione

Fanno parte della Commissione per l'aggiornamento e l'applicazione del Manuale di Gestione:

a) Il Segretario Generale;
b) Il Responsabile del Protocollo informatico
c) Il Responsabile Area Affari Generali
d) Il Responsabile dell'Ufficio Protocollo
e) Il Responsabile dei Sistemi Informatici
f) Il Responsabile della Sicurezza

o loro delegati.

Il Presidente della Commissione è il Segretario Generale. Il Vice Presidente è il Responsabile del Protocollo informatico.

13.6.2 Compiti della Commissione

I compiti della Commissione per l'aggiornamento e l'applicazione del Manuale di Gestione sono i seguenti:

a) realizzare sinergie con le strutture della Camera di Commercio in merito alla condivisione delle informazioni ricavabili dai documenti, dalla loro gestione e dalla loro conservazione;
b) esprimere un parere sul manuale, sul titolario di classificazione e sul massimario di selezione, nonché sulle loro eventuali modifiche;
c) proporre o redigere progetti speciali tendenti alla valorizzazione dei documenti della Camera di Commercio, alla conservazione, alla sicurezza dei locali di deposito e a quant'altro possa migliorare l'attività istituzionale inerente agli archivi;
d) proporre iniziative di formazione e aggiornamento professionale.

Allegati

1. Elenco delle abilitazioni
2. Criteri generali per l'inserimento delle anagrafiche dei referenti
3. Organigramma della Camera di Commercio
4. Manuale utente – Prodigi
5. Registro giornaliero di protocollo
6. Tabella dei procedimenti amministrativi
7. Titolario di classificazione
8. Massimario di selezione
9. Registro di emergenza
10. Camicia del fascicolo
11. Repertorio dei fascicoli
12. Glossario
13. Riferimenti normativi
14. Bibliografia essenziale

Allegato 1:

Elenco delle abilitazioni (strutture/persone e profilo utente associato)

Utenti abilitati al programma di protocollazione Proteus:

STRUTTURA	PERSONA	ABILITAZIONI

Allegato 2 Criteri generali per l'inserimento delle anagrafiche dei referenti.

INSERIMENTO ANAGRAFICHE DEI REFERENTI

Il programma Prodigi di Infocamere prevede l'implementazione di diverse anagrafiche finalizzate ad un controllo più efficace sulla qualità dei dati inseriti e ad una maggiore rapidità e precisione nei successivi inserimenti.

Le anagrafiche possono essere divise in due tipologie di referenti:

1. persone fisiche
2. enti/ditte

Per la predisposizione delle singole anagrafiche devono essere seguiti i seguenti criteri generali:

. i dati dell'anagrafica vanno ricavati direttamente dal documento in corso di protocollazione o, se necessario, da altri riferimenti disponibili legati in modo certo al documento (ad es. la busta che contiene il documento ricevuto)
. per l'inserimento dei dati si devono utilizzare le maiuscole e minuscole secondo l'uso corrente

1. Persone fisiche

. Per le persone fisiche si indica Cognome e Nome; eventuali titoli di cortesia, professionali o di onorificenza (professore, avvocato, architetto, geometra senatore ecc.), se indicati, dovrebbero seguire il cognome e nome.

2. Enti/ditte

. I nomi e le ragioni sociali devono essere sempre scritti in modo completo e per esteso (senza abbreviature e riportando gli articoli, preposizioni, virgolette. Ad es.: Camera di Commercio industria artigianato e agricoltura di Lecce e non Cam. Commercio di Lecce
. Le forme giuridiche come società per azioni, società a responsabilità limitata società cooperative etc.. si esprimono in forma abbreviata e senza puntini. Ad es. Spa – Srl- Scrl ecc.
. Qualora l'ente/ditta sia indicato anche attraverso una sigla o acronimo, questo deve essere inserito – in maiuscolo non puntato nell'anagrafica, dopo la denominazione dell'ente scritto per esteso e prima di ulteriori articolazioni.
Es.: Camera di commercio industria artigianato e agricoltura di Lecce – CCIAA Lecce
. Per le organizzazioni conosciute prevalentemente con la loro sigla (Es. INPS, CNR) si deve comunque inserire nell'anagrafica il nome esteso seguito dalla sigla.
Es.: Istituto Nazionale per la Previdenza Sociale – INPS
In ogni caso il sistema consente di risalire all'anagrafica corretta anche attraverso la ricerca di parti del testo.
(Es. per cercare Istituto Nazionale della Previdenza Sociale è sufficiente cercare INPS).
. Per gli enti e le organizzazioni il firmatario e la carica non si scrivono, perché non rilevanti ai fini della registrazione di protocollo.
. I nomi di enti/ditte estere si indicano nella lingua originale, indicando anche lo stato scritto in lingua italiana.
. Se un documento risulta privo dell'esatto indirizzo di provenienza o con una pluralità di indirizzi facenti riferimento a uffici o sedi amministrative, legali, operative, ecc., nell'anagrafica si dovrà indicare in ordine preferenziale: se sono presenti una sede legale e una sede operativa, quest'ultima.

Allegato 3: ORGANIGRAMMA DELLA CAMERA DI COMMERCIO di Lecce

La denominazione degli Uffici è indicativa degli stessi e l'organigramma sarà oggetto di aggiornamento in base all'evoluzione della struttura organizzativa.

Allegato 4: MANUALE UTENTE - PRODIGI

Allegato 5: REGISTRO GIORNALIERO DI PROTOCOLLO

Allegato 6: TABELLA DEI PROCEDIMENTI AMMINISTRATIVI

Si rinvia agli allegati del Regolamento camerale sul responsabile del procedimento amministrativo.

Allegato 7: TITOLARIO DI CLASSIFICAZIONE

dei documenti d'archivio delle Camere di Commercio

Allegato 8: MASSIMARIO DI SELEZIONE

Allegato 9: REGISTRO DI EMERGENZA

Allegato 10: COPERTINA DEL FASCICOLO (CAMICIA)

CAMERA DI COMMERCIO di _____

.....
(nome della struttura - divisione - ufficio)

Anno .....
Categoria ..... Classe ..... Sottoclasse
fascicolo n. ..... sottofascicolo ..... inserto .....

OGGETTO: .....

.....

.....

.....

.....

.....

Allegato 11: REPERTORIO DEI FASCICOLI

CAMERA DI COMMERCIO DI _____

REPERTORIO DEI FASCICOLI

ANNO _____

CATEGORIA _____ - _____

CLASSE	SOTTO-CLASSE	NUM. FASC.	SOTTO FASC.	INS.	OGGETTO	NOTE

Allegato 12: GLOSSARIO

Area Organizzativa Omogenea (AOO)
È un insieme definito di unità organizzative di una amministrazione che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare, ciascuna AOO mette a disposizione delle unità organizzative clienti il servzio di protocollazione dei documenti in entrata ed in uscita utilizzando una unica sequenza numerica, rinnovata ad ogni anno solare, propria alla AOO stessa. Di norma, l'AOO coincide, come nelle Camere di Commercio, con l'ente.

Casella istituzionale
La casella di posta elettronica istituita da una Area organizzativa omogenea (AOO) attraverso la quale vengono ricevuti i messaggi da protocollare (d.P.C.M. 31/10/2000 Art. 15 comma 3).

Fascicolo
Si tratta di un insieme organico di documenti relativi ad un medesimo affare o procedimento amministrativo, classificati in maniera omogenea. Si tratta quindi di un dossier, di una pratica, di una papèla, di una carpetta, etc.

Mezzo di corredo
È uno strumento tecnico predisposto dall'archivista per descrivere un archivio (o un fondo o una serie o comunque delle unità archivistiche): a secondo del grado di analisi e dello scopo per il quale viene approntato, può trattarsi di inventario, elenco di consistenza, elenco di versamento, indice, rubrica, ecc.

Piano di classificazione (v. titolario)

Responsabile del procedimento amministrativo (RPA)
È la persona fisica incaricata dell'istruzione e degli adempimenti di un affare o di un procedimento amministrativo.

Scarto (v. selezione)

Selezione dei documenti
Periodicamente e comunque prima del passaggio dei fascicoli alla sezione separata d'archivio devono essere effettuate le operazioni di selezione, cioè di individuazione dei documenti da destinare alla conservazione perenne o, qualora ritenuti inutili, allo scarto, cioè all'eliminazione fisica (per macero o termodistruzione).

Titolario di classificazione
Per titolario di classificazione si intende un quadro alfanumerico di riferimento per la formazione, gestione e conservazione dei documenti. Si tratta quindi di un sistema logico che suddivide i documenti secondo la funzione esercitata dall'ente che li produce, permettendo di organizzare in fascicoli secondo criteri omogenei i documenti che si riferiscono ad affari e a procedimenti amministrativi. Il titolario di classificazione delle Camere di Commercio si suddivide gerarchicamente in categorie, le quali si suddividono in classi e sottoclassi.

Unità organizzativa responsabile (UOR)
È l'ufficio (sezione, ripartizione, etc.), al quale afferisce il responsabile del procedimento amministrativo, previsto dall'art. 4 della legge 7 agosto 1990, n. 241.

Allegato 13: RIFERIMENTI NORMATIVI

Autorità per l'informatica nella Pubblica Amministrazione. *Deliberazione 30 luglio 1998, n. 24/98 - Regole tecniche per l'uso di supporti ottici*

Decreto legislativo 20 ottobre 1998, n. 368
Istituzione del Ministero per i beni e le attività culturali a norma dell'art. 11 della legge 15 marzo 1997, n. 59

Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999
Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novem.1997, n. 513

Decreto Legislativo 30 luglio 1999, n. 281
Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica

Direttiva del Presidente del Consiglio dei Ministri del 28 ottobre 1999
Gestione informatica dei flussi documentali nelle pubbliche amministrazioni

Decreto legislativo 29 ottobre 1999, n.490
Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000
Regole tecniche per per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428

Delibera dell'Autorità per l'informatica nella Pubblica Amministrazione 23 novembre 2000, n. 51
Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445
Testo unico sulla documentazione amministrativa

Decreto del Presidente della Repubblica 8 gennaio 2001, n. 37
Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato (n. 42, allegato 1, della legge n. 50/1999)

Autorità Garante per la protezione dei dati personali, Provvedimento 8/P/2001 del 14 marzo 2001
Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici

Allegato 14: BIBLIOGRAFIA ESSENZIALE

A. ANTONIELLA, *L'archivio comunale postunitario*, La Nuova Italia, Firenze 1979;

P. CARUCCI, *Le fonti archivistiche: ordinamento e conservazione*, Roma, NIS, 1983;

L. DURANTI, *I documenti archivistici. La gestione dell'archivio da parte dell'ente produttore, Ministero per i beni culturali e ambientali*, Roma 1997;

M.Guercio, *Manuale di archivistica informatica*, Carocci editore, Roma,2001;

E. LODOLINI, *Archivistica. Principi e problemi*, Milano, FAngeli, 1991 (ultima ed. 2001);

A. ROMITI, *I mezzi di corredo archivistici e i problemi dell'accesso*, in "Archivi per la Storia", III/2 (1990), pp. 217-246;

G. PENZO DORIA, *La linea dell'arco. Criteri per la redazione dei titolari di classificazione*, in Thesis 99. A*tti della 2^ Conferenza organizzativa degli archivi delle università italiane*, Padova, Cleup, 2001, pp. 305-340.

I. ZANNI ROSIELLO, *Archivi e memoria storica*, Bologna, Il Mulino, 1987

Letteratura Grigia

AUTORITÀ PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE, *Gedoc* : www.aipa.it
AUTORITÀ PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE, *Linee Guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali Gedoc 2* : www.aipa.it
SCUOLA SUPERIORE DELLA PUBBLICA AMMINISTRAZIONE, *Linee guida per la gestione informatica dei documenti:* http://www.sspa.it/