1214
CAMERA
DI COMMERCIO
INDUSTRIA ARTIGIANATO
AGRICOLTURA
LUCCA

Manuale di Gestione del Protocollo Informatico

Camera di Commercio, Industria, Artigianato e Agricoltura di LUCCA

Approvato con delibera di Giunta n. xx del xx/xx/xxxx

Versione x del xx/xx/xxxx

Sommario

Sezione I
Principi generali

1.1. Premessa

La proliferazione legislativa in materia di gestione documentale a cui abbiamo assistito negli ultimi anni ha contribuito a rendere tutti - amministratori ed operatori - più consapevoli dell'importanza strategica delle funzioni afferenti al protocollo. Al di là degli obblighi normativi introdotti, il vero cambiamento nasce e cresce all'interno di ogni singolo ente: dopo avere adottato un sistema di protocollo informatico e le prime versioni del manuale di gestione per far fronte a quanto previsto dal dpr 445/2000 e dal dpcm 31 ottobre 2000 l'Ente si trova a dover di nuovo intervenire sulla organizzazione dell'ente per recepire quanto previsto dalle modifiche apportate dal Codice dell'Amministrazione Digitale d. lgs. 82/2005 e da varie circolari ministeriali.
Le disposizioni sopra menzionate incidono infatti notevolmente sul contenuto del *Manuale*, in particolare per quanto attiene al valore dei documenti informatici.
Obiettivo del manuale è descrivere sia il sistema di gestione documentale a partire dalla protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio ma anche ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione, pertanto si rivolge non solo agli operatori di protocollo ma in generale a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

1.2 Definizioni e norme di riferimento

ai fini del presente manuale si intende per:
- Amministrazione o Camera: la Camera di Commercio Industria Artigianato Agricoltura di Lucca;
- Testo Unico: il dpr 445/2000;
- Codice Amministrazione Digitale (CAD): il d. lgs. 82/2005
- UOP – Unità Organizzative di registrazione di Protocollo – uffici che svolgono attività di registrazione di protocollo;
- UOR – Uffici Organizzativi di Riferimento – insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- UU – Ufficio Utente – ufficio che utilizza i servizi messi a disposizione dal sistema di protocollo informatico, ovvero il soggetto destinatario del documento;
- PEC – la Posta Elettronica Certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

1.3 Area Organizzativa Omogenea e modello organizzativo

Per la gestione dei documenti l'amministrazione ha individuato un'unica Area Organizzativa Omogenea (AOO) in quanto insieme definito di Unità che usufruiscono, in

modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. Essa è composta dall'insieme di tutti gli uffici articolati come riportato in allegato 1 (organigramma) . Nell'allegato sono indicati gli Uffici Utente e le Unità Organizzative di registrazione di Protocollo. All'interno dell'AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata presso l'Ufficio protocollo, mentre è decentralizzato per la corrispondenza in uscita, attraverso le UOR che svolgono anche i compiti di UOP.
L'allegato 1 è suscettibile di modifica in caso di inserimento di nuove Unità o di riorganizzazione delle stesse.
L'amministrazione si riserva la facoltà di autorizzare altre Unità allo svolgimento dell'attività di protocollazione, attività che dovrà comunque seguire le indicazioni del presente manuale e essere sottoposta al controllo del responsabile del protocollo informatico.

1.4 Servizio per la gestione informatica del protocollo

L'amministrazione ha provveduto all'istituzione del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi, alle dipendenze del Servizio Affari Generali e nell'ambito dell'Ufficio segreteria e protocollo, limitatamente al personale addetto alle funzioni di protocollazione.

Con determinazione n. 7 del 9/1/2006 è stata assunta direttamente dal Segretario Generale la responsabilità del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi.

E' compito del servizio:
- aggiornare lo schema del manuale di gestione del protocollo informatico;
- provvedere alla pubblicazione del manuale;
- aggiornare l'elenco dei documenti sottoposti a protocollazione particolare;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare gli addetti dell'amministrazione all'utilizzo del Prodotto di Protocollo informatico e definire, d'accordo con il responsabile dell'ufficio, il tipo di funzioni disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- curare le funzionalità del sistema affinché in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e comunque nel più breve tempo possibile;
- far conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il sistema;
- garantire il buon funzionamento degli strumenti ed il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza;
- registrare i protocolli riservati

1.5 Conservazione delle copie di riserva

Al fine di garantire la non modificabilità delle operazioni di registrazione il servizio procede alla stampa periodica e alla conservazione di copia cartacea del registro di protocollo.

1.6 Firma digitale

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione provvederà a fornire la firma digitale ai soggetti da essa delegati a rappresentarla.

1.7 Tutela dei dati personali

Per le misure adottate dall'amministrazione al fine di garantire la privacy ai sensi del d. lgs. 196/2003 si rimanda al dps e relativi allegati nonché ad ogni atto adottato dall'amministrazione in materia.

1.8 Caselle di posta elettronica

L'amministrazione dota tutti i propri dipendenti di una casella di posta elettronica.
L'Area Organizzativa Omogenea si è dotata della casella di posta elettronica certificata istituzionale camera.commercio.lucca@lu.legalmail.camcom.it per la corrispondenza in ingresso e in uscita, pubblicata sull'I.P.A. Si è inoltre dotata della casella tradizionale cameracommercio@lu.camcom.it per le comunicazioni che non sono destinate alla protocollazione e della casella

1.9 Sistema di classificazione dei d

L'amministrazione utilizza un unico titolario di classificazione ovvero 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.
Il titolario di classificazione adottato è stato elaborato per le Camere di Commercio 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 e integrato in alcune parti su indicazione del Responsabile del Protocollo Informatico e degli Archivi.
Il titolario di classificazione adottato è contenuto in allegato al presente manuale.

1.10 Formazione

L'amministrazione stabilisce percorsi formativi a favore del proprio personale in tema di gestione documentale e di protezione dei dati personali.

1.11 Accreditamento dell'amministrazione all'IPA

L'amministrazione, nell'ambito degli adempimenti previsti si è accreditata presso l'Indice delle Pubbliche Amministrazioni tenuto e reso pubblico dal CNIPA.

1.12 Procedure di conservazione sostitutiva

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si ha acquisito il prodotto Legaldoc di Infocert spa.

2 Introduzione del protocollo unico ed eliminazione dei protocollo interni

Con l'entrata in vigore del protocollo unico sono cessati di fatto e di diritto tutti i cosiddetti protocolli interni (cioè di settore, protocolli multipli, protocolli di telefax, ecc.) e tutti gli altri sistemi di registrazione dei documenti diversi dal protocollo unico.
Rimangono tuttavia in vigore il protocollo del Registro Imprese e i protocolli elencati nel cap. 8 del presente manuale in quanto soggetti a normativa separata.

2.1 Registro di protocollo

Il Registro di Protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso ed è idoneo a produrre effetti giuridici. Il Registro di Protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
Il Registro di Protocollo è gestito mediante sistema informatico.
La descrizione funzionale e operativa del sistema di protocollo informatico è costituita dal Manuale utente fornito dalla ditta fornitrice del sistema, aggiornato alla versione in uso.
Il Registro di Protocollo ha cadenza annuale: si apre al 1° gennaio e si chiude al 31 dicembre di ogni anno.
La numerazione è progressiva per anno.

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

3.1 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	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**				
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. Si rinvia a tal proposito a quanto descritto nel Documento Programmatico Sicurezza dell'Ente.

3.2 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.

3.2.1 Identificazione e Autenticazione (IA)

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

3.2.2 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 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

3.2.8 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.

3.3 Interventi operativi

3.3.1 Per i documenti informatici formati dalle applicazioni di InfoCamere s.c.r.l. e di Infocert s.p.a.

Per i documenti informatici formati conseguentemente all'utilizzo di applicazioni InfoCamere e di Infocert 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.

3.3.2 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 devono essere effettuati 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 intervento 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.

AC.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.

AC.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.

AC.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.

AC.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.

AC.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..

3.4 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).

3.4.1 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.

3.4.2 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 (3/4 mesi), password che deve avere dimensioni abbastanza significative (6/8 caratteri) in relazione al fatto che la difficoltà aumenta in maniera esponenziale con l'aumentare del numero dei caratteri usati e in ogni caso soddisfare le misure di sicurezza minime previste dalla vigente disciplina in materia di privacy laddove applicabile.

Ad ogni buon conto il responsabile dei sistemi operativi è la persona cui fare riferimento per ogni consiglio in merito.

3.4.3 Ulteriori accorgimenti.

3.4.3.1 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.

3.4.3.2 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.

3.4.3.3 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).

4 TIPOLOGIE DOCUMENTARIE E FLUSSO DI LAVORAZIONE DEI DOCUMENTI

4.1 Tipologie documentarie

Per documento amministrativo viene inteso ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale, così come prevede l'art. 22 comma 1 d) della legge 7 agosto 1990 , n° 241 così come modificata e integrata dalla LL. 15/2005 e 35/2005 .

Per documento informatico viene inteso qualsivoglia rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, così come prevede l'art. 1 del d. lgs. 82/2005.

I documenti si distinguono in documenti in arrivo, documenti in partenza e documenti interni. I documenti in arrivo e in partenza sono oggetto di registrazione di protocollo, ad esclusione dei documenti soggetti a registrazione particolare e dei documenti non soggetti a registrazione di protocollo.

4.2 Modalità di consegna dei documenti

Attualmente lo scambio di documenti può avvenire in cinque diverse modalità:

1. consegna a mano all'ufficio protocollo o agli sportelli;
2. spedizione postale tradizionale o con altri vettori;
3. fax;
4. posta elettronica;
5. PEC;
6. sistemi telematici dedicati quali Registro Imprese, Artigianato, Protesti, Mud, RAEE, Pile, Brevetti.

In particolare l'uso del telefax o di altro mezzo telematico o informatico idoneo ad accertare la fonte di provenienza del documento, soddisfa il requisito della forma scritta per cui la trasmissione dei documenti con tali strumenti non deve essere seguita da quella del documento cartaceo originale (art. 38.1 e 43.6 del DPR 445/2000), a meno che non si tratti di un documento contabile (fattura, notula etc.) che, per il valore fiscale che assume, è buona prassi che sia conservato dall'Ente in originale o di documenti per i quali la legge prevede una forma particolare per la notificazione degli atti amministrativi.

4.2.1 Scambio di documenti informatici e utilizzo della posta elettronica

Ai sensi dell'art. 20 del Codice, come successivamente modificato, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e' liberamente valutabile in giudizio, fermo restando che il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, si presume riconducibile al titolare del dispositivo di firma e soddisfa comunque il requisito della forma scritta. Ai sensi dell'art. 65 del CAD l'istanza è altresì valida quando l'autore e' identificato dal sistema informatico attraverso le credenziali di accesso relative all'utenza personale di posta elettronica certificata o attraverso un sistema di identificazione informatica che rilascia le credenziali solo dietro la presentazione di una copia di un documento d'identità.

Il messaggio di posta elettronica ordinaria non soddisfa invece di per sé il requisito della forma scritta, quindi non ha la stessa efficacia probatoria del documento cartaceo sottoscritto mediante la sottoscrizione autografa o del documento informatico sottoscritto mediante firma elettronica, anche in considerazione del fatto che il messaggio di posta elettronica può essere facilmente contraffatto e modificato. Pertanto è possibile la protocollazione di un messaggio di posta elettronica ordinaria in entrata solo se è allegato da copia di documento di riconoscimento. Quanto alla data, farà fede quella di registrazione da parte del UOP.

Poiché l'integrità del messaggio è condizione imprescindibile per lo svolgimento dell'azione amministrativa, al fine di attestare o documentare un atto, un fatto, uno stato o una qualità, il responsabile del procedimento amministrativo deve pretendere dal corrispondente un documento sottoscritto, tradizionalmente o informaticamente, dando adeguata informativa al mittente del messaggio.

Nel caso di semplici richieste di informazioni è possibile rispondere a mezzo email non protocollata.

4.3 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.

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. A tal fine il responsabile del procedimento amministrativo che produce un documento interno, lo invia all'ufficio protocollo per le operazioni di registrazione degli elementi obbligatori e degli elementi accessori del protocollo.
L'ufficio protocollo provvede all'assegnazione del documento in competenza all'UOR destinataria e in conoscenza all'UOR mittente.
L'ufficio protocollo provvede alla registrazione del documento interno, di norma entro il medesimo giorno lavorativo.
La gestione archivistica del documento (fascicolazione e gestione del fascicolo) verrà effettuata dal responsabile del procedimento (destinatario).

4.4 Documenti in partenza

Per documento in partenza si intende ogni documento prodotto dal personale in servizio presso la Camera di Commercio nell'esercizio delle proprie funzioni avente rilevanza giuridico probatoria e diretto all'esterno (destinatari esterni all'ente).

Oltre ai documenti in forma cartacea, ad oggi la Camera di Commercio può inviare a destinatari esterni alcune tipologie di documenti informatici.

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

a) Sigillo e logo della Camera di Commercio e dicitura "Camera di Commercio di ... ";

b) indirizzo completo della Camera di Commercio (via, numero, c.a.p., città, provincia);
c) numero di telefono;
d) numero di telefax;
e) indirizzo di posta elettronica e del sito web;
f) data completa (giorno, mese, anno);
g) numero di protocollo;
h) numero degli allegati, se presenti;
i) UOR;
j) destinatario;
k) oggetto del documento;
l) firma autografa, o informatica (digitale) del responsabile/referente o scansione della firma in caso di semplice comunicazione purché corrispondente a quella depositata nello specimen

4.4.1 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, perfetta e autentica negli elementi sostanziali e formali. L'originale del documento è unico, salvo i casi dove è previsto un originale multiplo (contratti, convenzioni, ecc….) o i casi in cui si renda necessario produrre per il medesimo procedimento sia un originale analogico che un originale digitale (tale situazione si verifica ad esempio per la convocazione della Giunta e del Consiglio, che viene effettuata per alcuni membri con trasmissione di documento informatico tramite PEC e per alcuni membri tramite trasmissione del documento analogico via fax).
L'originale del documento va di norma spedito.
Sia l'originale sia la minuta vanno corredati di firma autografa o informatica.
Per minuta si intende l'originale del documento da conservare "agli atti" con la dicitura "minuta", cioè nel fascicolo relativo all'affare o al procedimento amministrativo trattato.
Qualora si renda necessario per ragioni amministrative, si possono produrre copie di un medesimo documento.
Qualora ci siano più destinatari, è autorizzata la spedizione di copie dell'originale. In questo caso, la registrazione di protocollo, che sarà unica, riporterà il primo nominativo o la descrizione dei destinatari e l'elenco dei destinatari dovrà essere conservato in allegato alla minuta.
Nel caso di spedizione di un documento tramite la PEC, è consentito l'invio di una riproduzione informatica dell'originale cartaceo sottoscritto con firma autografa o digitale o scansione di firma autografa, esclusivamente nei formati PDF, TXT, XML. Sono fatti salvi i ad esclusione dei casi in cui la legge preveda una forma particolare per la notificazione degli atti amministrativi. In tal caso, l'originale cartaceo, riprodotto informaticamente a cura dello stesso ufficio produttore, viene conservato agli atti con la dicitura "ORIGINALE RIPRODOTTO INFORMATICAMENTE ".

4.4.2 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronica/digitale conforme alle disposizioni dettate dalla normativa vigente, utilizzando i servizi di riconoscimento e autenticazione disponibili sulla rete della Camera di Commercio. Indipendentemente dal software utilizzato, prima della loro

sottoscrizione con firma elettronico/digitale, laddove prevista, i documenti sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.
In caso di semplici comunicazioni è sufficiente apporre in calce al documento informatico la scansione della firma del referente/responsabile.

4.4.3 Registrazione e spedizione dei documenti in partenza

La trasmissione dei documenti all'esterno dell'ente può avvenire per mezzo del servizio postale (posta prioritaria, raccomandata, etc.), per mezzo di corrieri o via fax per i documenti analogici, nonché tramite posta elettronica o PEC per i documenti informatici.

A meno che la normativa specifica non richieda un mezzo di trasmissione diverso, l'invio dei documenti, ai sensi degli articoli 5 bis e 6 del Codice dell'Amministrazione Digitale, dovrà avvenire per via informatica (email semplice o pec) nel caso di pubbliche amministrazioni, soggetti che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata, imprese che hanno comunicato il proprio indirizzo email. Non è comunque possibile imporre l'uso delle tecnologie della comunicazione e dell'informazione alle imprese per lo scambio di comunicazioni con la pubblica amministrazione a meno fino a quando non termina il periodo di transizione per l'acquisizione della posta elettronica certificata. La scelta del mezzo di trasmissione più opportuno, quando non espressamente indicato dalla normativa vigente, spetta al responsabile del procedimento amministrativo. Egli dovrà tuttavia tenere conto di due obblighi normativi:

1- in base a quanto previsto all'art. 6 del Codice dell'Amministrazione Digitale (CAD), ai soggetti che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata i documenti dovranno essere trasmessi tramite PEC;
2- in base a quanto previsto dall'art 5 bis del Codice dell'Amministrazione Digitale "la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione". Tale norma

Come specificato al punto 1.3 la protocollazione in uscita è decentralizzato in molti uffici, indicati in allegato 1 come UOP.

Gli U.O.R. che non effettuano protocollazione in uscita, una volta prodotto il documento in partenza, lo registrano e lo inviano all'ufficio protocollo. L'ufficio Protocollo, dopo avere effettuato la registrazione, di norma entro il giorno lavorativo successivo alla consegna da parte dell'ufficio produttore, riconsegna la minuta all'ufficio che ha prodotto il documento e spedisce l'originale per posta o lo riconsegna all'ufficio produttore per la eventuale spedizione del fax. In questi casi il documento in partenza viene scansionato a fini esclusivamente gestionali.
Qualora il documento debba essere trasmesso tramite PEC o fax, il soggetto sottoscrittore del documento, dopo aver fatto registrare registrato il documento al Protocollo, potrà trasmettergli: procederà all'invio:
- il file del file o dei files relativo/i alla scansione del documento/i originale/i con firma autografa e con la dicitura "ORIGINALE RIPRODOTTO INFORMATICAMENTE";
- il del file firmato elettronicamente/digitalmente o con scansione della firma del responsabile/referente.
È possibile l'invio di file tramite PEC solo in formato PDF, TXT, XML.

Il Protocollo L'UOR procede quindi successivamente alla trasmissione della PEC all'indirizzo indicato dall'ufficio e all'invio in conservazione tramite Legaldoc.

Nel caso di documenti in uscita protocollati da altri uffici che svolgono le funzioni di UOP, essi, dopo aver prodotto e registrato il documento, e avere associato al protocollo creato il file, provvedono direttamente alla spedizione tramite fax oppure procedono, secondo una delle modalità di seguito indicate, alla trasmissione al protocollo:
- i I documenti che devono essere trasmessi tramite posta devono essere consegnati all'UOP entro le ore 10.30, al fine di procedere con l'espletamento delle operazioni richieste. all'affrancatura e alla consegna all'ufficio postale nei tempi da esso richiesti;
- per i documenti che devono essere trasmessi tramite PEC, l'ufficio produttore del documento trasmette una mail di richiesta al Protocollo con indicazione dell'indirizzo di PEC del destinatario, e del numero di protocollo relativo al documento da trasmettere.
I file relativi ai documenti in partenza vengono associati al protocollo creato direttamente dall'ufficio produttore con finalità esclusivamente gestionali nel caso di invio tramite posta/corriere/fax; qualora invece il documento venga trasmesso tramite PEC, l'ufficio che ha registrato il documento dovrà procedere direttamente anche all'invio in conservazione tramite Legaldoc.

La posta in uscita viene di norma spedita il giorno lavorativo in cui è stato protocollato.

In ogni caso la gestione archivistica del documento (fascicolazione e gestione del fascicolo) verrà effettuata dal responsabile del procedimento.

4.5 Documenti in arrivo

Essi possono essere o documenti cartacei (analogici) o files pervenuti con una delle modalità di cui al punto 4.2.
La Camera di Commercio si riserva di trattare i documenti informatici che l'attuale dotazione tecnologica gli permette di leggere e decodificare.
L'originale del documento (sia in formato digitale che analogico), dopo le operazioni di protocollazione, va di norma inviato al responsabile del procedimento amministrativo.

4.5.1 Procedure per la ricezione dei documenti cartacei

I documenti in arrivo tramite posta, devono pervenire all'ufficio preposto all'apertura della corrispondenza entro le ore 9.30 in modo da garantire l'efficienza della registrazione.
La corrispondenza in arrivo, di norma, va infatti aperta e protocollata nel medesimo giorno lavorativo di ricezione. In particolare il personale dell'Ufficio Segreteria e Protocollo addetto alla protocollazione, provvede ad aprire tutta la corrispondenza ad eccezione di quanto specificato al successivo punto 4.5.2, a protocollare i documenti e registrarli (punto 4.5.3), a smistarli alle unità organizzative competenti e a scansionarli (punto 4.5.4).
Presso il Servizio Registro Imprese Albo Artigiano Rec Albi e Ruoli alcune pratiche vengono protocollate direttamente dal responsabile o dagli addetti dell'ufficio competente mediante il programma Workflow sull'applicazione Prodigi. Poiché tale programma non consente l'assegnazione del protocollo, la responsabilità del procedimento delle pratiche così ricevute e protocollate viene assunta dal protocollatore

della pratica. Le pratiche in arrivo protocollate dagli uffici di tale Servizio vengono fatte pervenire all'Ufficio protocollo al solo fine della scansione.

4.5.2 Documenti in arrivo da non aprire

La corrispondenza non viene aperta dal personale addetto alla protocollazione nei seguenti casi:

a) corrispondenza riportante l'indicazione, "concorso" o "gara d'appalto" o simili: tale corrispondenza non viene aperta ma viene protocollata la busta poi inoltrata direttamente all'unità organizzativa responsabile del procedimento amministrativo;
b) corrispondenza indirizzata nominativamente (senza indicazione dell'ente) oppure riportante l'indicazione "riservata", "personale" o simili, o comunque dalla cui confezione si evinca il carattere di corrispondenza privata: tale corrispondenza viene inoltrata direttamente al destinatario.
c) corrispondenza indirizzata al Presidente e/o al Segretario Generale: tale corrispondenza viene aperta dal personale addetto alle funzioni di segreteria, che provvede a fornire le indicazioni per il successivo smistamento e protocollazione.

4.5.3 Registrazione di un documento in arrivo

La registrazione del documento in arrivo avviene attraverso l'assegnazione dei seguenti elementi:

a) data di registrazione
b) numero di protocollo
c) mittente
d) oggetto
e) data e numero del protocollo del documento in arrivo (se disponibili)
f) classificazione
g) impronta del documento (quando viene protocollato un documento informatico)
h) mezzo di ricezione (eventuale).

L'assegnazione delle informazioni nelle operazioni di registrazione è effettuata dal sistema di protocollazione informatico in un'unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.

4.5.4 Scansione ottica dei documenti

La Camera utilizza l'archiviazione ottica dei documenti in arrivo, a fini esclusivamente gestionali, e non con finalità sostitutive dell'originale. Pertanto le copie dei documenti riprodotti tramite scanner non hanno, al momento, alcun valore legale e probatorio, non sono cioè assimilabili alle copie conformi.
In casi eccezionali di documenti formati da molte pagine l'ufficio protocollo procede alla scansione parziale.

4.5.5 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 è autorizzato a rilasciare una ricevuta stampata dal sistema informatico per la gestione del protocollo che riporti i dati della registrazione del documento.
Solo nel caso in cui non sia possibile protocollare subito il documento, l'ufficio protocollo è autorizzato ad apporre su una copia della prima pagina del documento il timbro di arrivo con la data di arrivo e la sigla dell'operatore.

4.5.6 Ricezione di documenti tramite fax

Il fax arriva su Prodigi come riproduzione digitale di un documento analogico. Il sistema classifica il fax ricevuto come un documento informatico e l'UOP provvede alla registrazione. In tale fase l'UOP deve prestare attenzione a che il fax venga registrato effettivamente come documento principale e in caso contrario provvede a modificare il protocollo e ad effettuare l'inversione tra il documento principale e l'allegato.
Una volta registrato, il fax come documento informatico viene smistato all'ufficio competente il quale sarà responsabile dell'archiviazione dello stesso secondo il massimario di scarto.
Il protocollatore nella registrazione di protocollo del fax ricevuto, di norma, dovrà indicare il mezzo di ricezione "fax" nell'apposito campo della maschera di inserimento dei dati. Del ricevimento dei fax all'apparecchio collocato presso l'Ufficio Protocollo, viene data notizia all'ufficio destinatario anche tramite posta elettronica.
La segnatura di protocollo sarà apposta sulla copertina di trasmissione.
Qualora venga successivamente ricevuto lo stesso documento tramite posta il protocollatore, accertato che si tratta del medesimo documento già pervenuto via fax e protocollato, annota sul documento pervenuto tramite posta le informazioni relative al precedente protocollo. Il responsabile del procedimento amministrativo conserva il documento cartaceo ricevuto tramite posta con il fax protocollato nel fascicolo.
I fax che avranno ad oggetto dichiarazioni sostitutive saranno accettati solo se allegati da fotocopia di un documento di riconoscimento. Una volta ricevuto il fax, l'UOP provvede a protocollarlo, assegnarlo all'ufficio competente e a trasmettere la ricevuta di protocollo a detto ufficio.
Analogamente, qualora vengano attribuiti due numeri di protocollo allo stesso documento ricevuto sia tramite fax che per posta, il responsabile del procedimento deve conservare entrambi i documenti.

4.5.7 Ricezione di documenti informatici tramite posta elettronica

Attualmente la protocollazione dei documenti informatici pervenuti tramite posta elettronica viene effettuata attraverso la posta elettronica certificata camera.commercio.lucca@lu.legalmail.camcom.it, che attualmente è l'unica casella collegata al sistema Prodigi, in quanto l'inserimento nel sistema di protocollo informatico di una ulteriore casella istituzionale costituirebbe un inutile aggravio per l'ufficio. Per questo motivo si ritiene per il momento utile lasciare aperta la casella PEC anche alla posta elettronica ordinaria, prevedendo che eventuali messaggi pervenuti sulla casella PEC ma che non debbono essere protocollati potranno essere cancellati.

Quando i documenti pervengono alla casella di posta elettronica certificata direttamente dall'esterno, l'ufficio protocollo, eventualmente previa verifica della validità della firma apposta, nonché della leggibilità e della possibilità di inviare in conservazione sostitutiva il documento, procede alla registrazione di protocollo, allo smistamento dello stesso e alla trasmissione della ricevuta di protocollo all'ufficio.

L'assegnatario del protocollo deciderà se stampare il documento informatico: in questo caso la stampa avrà il semplice valore di una riproduzione.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente.

Come già specificato al punto 4.2.1, qualora i documenti non siano dotati di firma elettronica, la loro valenza giuridico probatoria è assimilabile a quella di una missiva non sottoscritta e comunque valutabile solo dal responsabile del procedimento amministrativo, pertanto:
- qualora il responsabile del procedimento ritenga opportuno attribuire ad un messaggio ricevuto sulla propria casella di posta elettronica efficacia probatoria, provvede a trasmetterlo inoltrarlo alla casella istituzionale certificata, inserendolo così nel sistema di gestione documentale con il formato di origine quindi il protocollo provvede a protocollarlo, smistarlo, assegnarlo, gestirlo e a trasmettere la ricevuta di protocollo all'ufficio;
- qualora pervenga dall'esterno un messaggio da una casella di posta elettronica non certificata e/o contenente un documento non firmato elettronicamente/digitalmente il personale addetto alla protocollazione, qualora non rilevi che il documento è già pervenuto tramite altra modalità o che si tratta di documenti non soggetti a registrazione (punto 6), provvede a protocollarlo e assegnarlo all'ufficio competente e a trasmettere la ricevuta di protocollo all'ufficio; il responsabile del procedimento assegnatario del protocollo provvederà eventualmente, come specificato al punto 4.2.1, a pretendere dal corrispondente un documento sottoscritto, tradizionalmente o informaticamente, dando adeguata informativa al mittente del messaggio.
I messaggi di posta elettronica che hanno ad oggetto dichiarazioni sostitutive saranno accettati solo se allegati da fotocopia di un documento di riconoscimento. Una volta ricevuto il messaggio di posta elettronica, l'UOP provvede a protocollarlo, assegnarlo all'ufficio competente e a trasmettere la ricevuta di protocollo a detto ufficio.
Anche in questo caso l'assegnatario del protocollo deciderà se stampare il documento informatico: in questo caso la stampa avrà il semplice valore di una riproduzione.

Qualora, a causa di problemi tecnici di compatibilità tra il provider del mittente e prodigi, non sia possibile aprire la PEC ricevuta occorre procedere seguendo i sottoelencati passaggi:

- salvare il file sul proprio PC;
- registrare il messaggio di PEC;
- associare al messaggio di PEC registrato il file precedentemente salvato sul desktop.

4.5.8 Conservazione dei documenti nell'archivio corrente

L'U.O.R. di assegnazione del documento provvede alla verifica della classificazione attribuita dall'ufficio protocollo e alla successiva fascicolazione del documento, nonché alla conservazione dei fascicoli attivi.

4.6 Utilizzo del programma Legaldoc

Attualmente la Camera utilizza il programma Legaldoc per l'invio in conservazione sostitutiva dei documenti informatici, con esclusione dei file di origine dei documenti analogici spediti e dei file risultanti dalla scansione dei documenti analogici in arrivo come specificato al punto 4.5.4.

Come previsto dall'attuale contratto con Infocert, al momento dell'invio in conservazione in Legaldoc, il protocollatore indica quale periodo di conservazione 5 anni, 10 anni o permanente attenendosi a quanto previsto dal massimario di scarto.
L'attuale contratto prevede la possibilità di conservare i file con i formati .pdf, .tif, .txt, .xml, .jpg, .doc, .xls, .rtf, .ppt, .zip, .html, tuttavia, in considerazione della necessità di prediligere i file con minore possibilità di essere modificati, con comunicazione di servizio del 2008 è stato chiesto al personale della Camera di far protocollare solo file con i formati .txt, .pdf, .xml.
Il programma prevede inoltre una serie di limitazioni tecniche (ad esempio gli allegati non devono superare i 50 file, i nomi dei file contenuti nel messaggio non devono contenere più di 60 caratteri e devono contenere solo cifre e lettere dell'alfabeto inglese, la dimensione massima di ciascun file allegato al messaggio non deve superare i 2Mb) che possono rendere necessario richiedere alcuni particolari accorgimenti all'utenza.
Tali limitazioni comportano inoltre la necessità da parte degli addetti alle funzioni di protocollo di adottare alcuni accorgimenti, quali, ad esempio:
- temporaneo salvataggio del file e successiva "associazione del file" al protocollo;
- intervento sui campi "mittente" e "oggetto" prodotti automaticamente dal sistema prodigi nel caso di inoltro alla PEC di un messaggio email: il sistema inserisce infatti nel campo "mittente" l'indirizzo email del soggetto che ha inoltrato il messaggio e nel campo "oggetto" "fwd..oggetto della email"; per agevolare la ricerca del protocollo si interviene sia nel campo mittente indicando la denominazione del mittente, che nel campo oggetto al fine di dare una chiara definizione dell'oggetto.

5 REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI

L'attività di smistamento consiste nell'operazione di inviare un documento protocollato e segnato all'U.O.R. competente. Con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico ed alla trasmissione del materiale documentario oggetto di lavorazione.
La responsabilità del procedimento di protocolli non assegnati resta in carico al protocollatore.
Chiunque si accorga di aver ricevuto per errore tra la propria corrispondenza un documento inerente a procedimenti relativi ad altra unità organizzativa responsabile, deve tempestivamente consegnare o far pervenire l'originale cartaceo a colui che gliel'aveva assegnato e parimenti rinviargli informaticamente il documento.
Il destinatario della comunicazione è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento passando nella fase "letto" il protocollo.
L'applicazione di protocollo informatico tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

5.1. Smistamento e assegnazione di competenza dei documenti ricevuti in formato cartaceo

Fermo restando quanto indicato al punto 4.5.1 per le pratiche del Servizio Registro Imprese Albo Artigiano Rec Albi e Ruoli che vengono protocollate direttamente dal responsabile o dagli addetti dell'ufficio competente mediante il programma Workflow e che non vengono assegnate, tutti gli altri documenti in arrivo, terminate le operazioni di registrazione, segnatura, scansione e assegnazione sono trasmessi all'U.O.R. tramite l'applicazione di protocollo informatico e in originale cartaceo.

Qualora un documento tratti più argomenti, imputabili a procedimenti amministrativi o affari diversi, verrà individuato un U.O.R. di competenza, cui viene trasmesso il documento in originale e tramite l'applicazione di protocollo informatico, e più U.O.R. cui viene trasmesso per conoscenza tramite l'applicazione del protocollo informatico e eventualmente una copia dell'originale .
La posta aperta direttamente dall'ufficio Protocollo viene assegnata in competenza dall'ufficio Protocollo stesso (attraverso l'applicazione del protocollo informatico e il recapito del cartaceo) all'Unità Organizzativa Responsabile del procedimento amministrativo (Dirigente/Servizio/Ufficio) individuando gli assegnatari dal testo del documento.
Per la posta aperta direttamente dall'ufficio Segreteria (documenti indirizzati al Segretario Generale e al Presidente), lo stesso ufficio Segreteria o se necessario il Segretario Generale o il Presidente provvede ad indicare all'ufficio Protocollo le assegnazioni in competenza all'U.O.R. .
Il dirigente o responsabile del servizio (o un loro incaricato) provvedono, se necessario, ad assegnare ciascun documento in arrivo loro smistato dall'ufficio Protocollo al responsabile del procedimento amministrativo.
Inoltre ogni documento può essere inviato in conoscenza ad altri settori od uffici.
Qualora venga erroneamente registrato un documento di competenza di terzi (altro ente, altra persona fisica o giuridica), la registrazione va annullata.

5.2 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'A.O.O. per via telematica non soggetti a registrazione particolare sono assegnati all'U.O.R. dall'Ufficio protocollo, fermo restando quanto riportato al punto 4.5.1, al termine delle operazioni di registrazione e segnatura. L'Ufficio protocollo trasmette quindi una stampa cartacea della sola registrazione e l'ufficio deciderà se stampare il documento al fine di inserirlo nel relativo fascicolo cartaceo. L'U.O.R. può comunque visualizzare il documento informatico tramite il programma di protocollazione.

5.3 Casi particolari di assegnazione di documenti in arrivo

Con l'introduzione del protocollo informatico la Camera di Commercio di Lucca ha approfondito e razionalizzato i flussi documentali dei documenti.
Per la maggior parte di essi si è trattato semplicemente di confermare prassi già in vigore e perfettamente conformi alla normativa. Per alcune categorie, invece, è stato opportuno effettuare alcune modifiche, al fine di una corretta gestione, fascicolazione ed archiviazione dei documenti stessi.
In particolare, la razionalizzazione del flusso documentale ha interessato:

1. fatture;
2. preventivi di spesa;
3. comunicazioni di interesse di più settori contemporaneamente;
4. comunicazione dei corsi di formazione;
5. circolari;
6. sentenze di fallimento;
7. fondi di perequazione;
8. partecipate.

1. FATTURE

Bisogna distinguere tra le varie tipologie di fatture, in quanto a seconda del fornitore o dell'oggetto cambia anche la gestione del documento e, quindi, l'assegnazione per competenza.
L'ufficio protocollo attribuisce:

a) Le bollette di pagamento (utenze), i Viacard, i Postel, le cartelle esattoriali:
Per competenza -> ufficio ragioneria

b) Le fatture di Infocamere e di Infocert
Per competenza -> Claudio Mori

Tutte le altre fatture sono attribuite dall'ufficio protocollo per competenza all'ufficio provveditorato.
Ai protocolli relativi a tutte le fatture, con l'esclusione solo delle fatture di cui al punto precedente a) e relativi a tutte le note di credito, viene apposta la dicitura "pubblico" del sistema Prodigi, al fine di permettere la gestione delle stesse tramite l'applicativo XAC di Infocamere e il conseguente acceleramento dei tempi "di lavorazione" della fattura stessa.

2. PREVENTIVI DI SPESA

L'ufficio protocollo, accertato l'ufficio richiedente il preventivo, lo smista per competenza all'ufficio stesso

3. COMUNICAZIONI DI INTERESSE DI PIÙ SETTORI CONTEMPORANEAMENTE

Si tratta, ad esempio, di alcune note di Unioncamere, di InfoCamere, del ministero etc… che in genere non danno luogo all'avvio di un procedimento.
Vengono protocollate:
Per competenza -> ufficio segreteria;
Per conoscenza -> tutti gli altri uffici, servizi o dirigenti interessati.

4. COMUNICAZIONE DEI CORSI DI FORMAZIONE DI INTERESSE DI PIU' SETTORI CONTEMPORANEAMENTE

Per competenza -> ufficio personale;

5. CIRCOLARI

Le circolari vengono attribuite per competenza ai dirigenti interessati

6. SENTENZE DI FALLIMENTO

L'ufficio protocollo le attribuisce:
per competenza -> ufficio registro imprese
per conoscenza -> ufficio artigianato, ufficio diritto annuale, ufficio rec - albi e ruoli, ufficio settori produttivi, ufficio sanzioni, ufficio statistica.

7. FONDO DI PEREQUAZIONE

L'ufficio protocollo attribuisce:

a) comunicazioni generali:
Per competenza -> ufficio segreteria e protocollo
Per conoscenza ->altri possibili interessati (dirigenti, capo servizio, uffici)

b) comunicazioni sui singoli progetti:
Per competenza -> ufficio competente
Per conoscenza -> ufficio segreteria e protocollo

c) comunicazioni su acconti e saldi
Per competenza -> ufficio ragioneria
Per conoscenza -> ufficio segreteria e protocollo

8. PARTECIPATE

Per competenza -> segreteria

6 ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

I documenti per i quali non è prevista la registrazione di protocollo sono:

- lettere anonime
- lettere prive di destinatario
- gazzette ufficiali
- bollettini ufficiali
- notiziari della pubblica amministrazione
- note di ricezione delle circolari e altre disposizioni
- materiali statistici (ad esclusione di quanto protocollato dal mittente)
- atti preparatori interni
- estratti conto bancari e postali
- giornali
- riviste
- libri
- materiali pubblicitari
- inviti a manifestazioni
- documenti di interesse effimero (ringraziamenti, congratulazioni, condoglianze, ecc…)
- tutti i documenti già soggetti a registrazione particolare dall'amministrazione.

I documenti soggetti a registrazione particolare sono individuati dal dirigente di unità organizzativa responsabile in collaborazione con il responsabile del protocollo informatico.

7 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

7.1 Serie delle Delibere e delle Determinazioni e rispettivo repertorio generale

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.

Ciascun complesso delle delibere e delle determinazioni costituisce una serie:
a) delibere di Giunta
b) delibere di Consiglio
c) determinazioni del Presidente
d) determinazioni del Segretario Generale e dei Dirigenti

All'interno di ciascuna serie, ogni delibera/determinazione ha un proprio numero di repertorio con numerazione annuale, che inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Presso la Segreteria sono conservate le serie relative agli ultimi cinque anni. Le serie esaurite da oltre cinque anni vanno versate all'archivio di deposito.
Per ogni delibera e determinazione deve essere prodotto un solo originale, ferme restando le copie dichiarate conformi e le copie di carattere informativo riprodotte per le esigenze d'ufficio.

7.2 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 della Segreteria Generale.
L'originale va conservato nella rispettiva serie (serie delle delibere, serie delle determinazioni) e ordinato secondo il numero di repertorio.

7.3 Denunce all'ufficio Registro delle Imprese

Le seguenti tipologie di documento:
a) le domande di iscrizione, modifica o cancellazione dal R.I. sia quelle presentate allo sportello che quelle inviate per posta o in via telematica nonché le notifiche di iscrizione, modifica o cancellazione dal R.I.
b) le denunce del R.E.A. sia quelle presentate allo sportello che quelle inviate per posta o in via telematica
c) la vidimazione dei libri contabili
d) i verbali e le notifiche di sanzione amministrativa
sono soggette a registrazione particolare.
Tutte le altre tipologie di documento, quali, ad es.:
a) le richieste di regolarizzazione relative a domande Registro Imprese e denunce R.E.A.;

b) la risposta alle richieste di regolarizzazione da parte dei diretti interessati;
c) le richieste di visure/certificati/elenchi inviate per posta/fax;
d) l'invio di visure/certificati/elenchi richiesti per posta/fax;
e) le richieste di controlli agli Enti preposti;
f) le richieste di certificazioni e attestazioni per leggi speciali;
g) informative varie;
h) le richieste di accertamento sui requisiti di onorabilità (e le relative risposte)
i) le notifiche di iscrizione, modifica o cancellazione dal R.I./R.E.A. nonché di rifiuto o di archiviazione a fronte di richieste presentate tramite postA, allo sportello o in via telematica

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

7.4 Protesti Cambiari

Le seguenti tipologie di documento:
a) l'elenco Protesti consegnato dall'Ufficiale Levatore, preventivamente registrato
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.

Tutte le altre tipologie di documento, quali, ad es.:
a) le comunicazioni di avvenuta cancellazione
b) le comunicazioni di avvenuta annotazione

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

7.5 Domande di Brevetti e Marchi

Le seguenti tipologie di documento:
a) domande relative a marchi
b) domande relative a brevetti (invenzioni, modelli di utilità, modelli ornamentali)
c) seguiti (annotazioni varie, trascrizioni) e istanze
d) tasse

sono soggette a registrazione particolare da parte dell'Ente.

Tutte le altre tipologie di documento, quali, ad es., l'invio delle domande di brevetto al MICA non sono soggette a registrazione particolare da parte dell'Ufficio, e vengono registrate nel protocollo generale dell'Ente.

7.6 M.U.D.

I modelli di dichiarazione ambientale (Mud) sono soggette a registrazione particolare da parte dell'Ufficio.

7.7 Fatture

Le fatture emesse dall' Ente sono sottoposte a registrazione particolare da parte dell'ufficio Provveditorato e degli uffici erogatori del servizio.

Le fatture ricevute dall'Ente non sono soggette a registrazione particolare da parte dell'Ufficio Ragioneria ma vengono registrate nel protocollo generale dell'Ente.

7.8 Sanzioni

I verbali di accertamento di infrazioni amministrative che arrivano all'ufficio Sanzioni sono sottoposte a registrazione particolare da parte dell'ufficio stesso

7.9 Albo Artigiani

a) le domande di iscrizione, modifica o cancellazione dall'albo artigiani sia quelle presentate allo sportello che quelle inviate per posta o in via telematica nonché le notifiche di iscrizione, modifica o cancellazione dall'albo artigiani e le richieste di regolarizzazione a fronte di richieste presentate in via telematica.
b) richieste di iscrizioni o cancellazioni di collaboratori familiari (sia per posta che per sportello che telematica)
c) protocollazione qualifiche professionali parrucchieri
d) verbale e notifica di sanzione amministrativa

8 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

L'ufficio protocollo e gli U.O.P. per i documenti protocollati autonomamente, attribuiscono la classificazione secondo il titolario di cui al punto 1.9.

8.1 Il fascicolo: individuazione, gestione e tenuta

Attualmente la Camera di Commercio di Lucca gestisce i fascicoli cartacei e l'archivio. Ogni ufficio predispone i fascicoli cartacei per i procedimenti di propria competenza, ma al momento non sono ancora stati definiti criteri di uniformità per l'identificazione (anno, indice di classificazione, nr.) dei fascicoli e per la formazione dei mezzi di corredo (repertorio ecc…).
Attualmente, l'assegnatario del documento provvede ad una prima archiviazione dello stesso, secondo le seguenti regole:

- per ciascuna pratica è previsto un unico raccoglitore contenente tutti i documenti che la riguardano e ben identificabile;
- è inserito all'inizio del raccoglitore un elenco di tutti i documenti contenuti nello stesso;
- i documenti, all'interno del raccoglitore, sono suddivisi in categorie e inseriti in ordine cronologico.

8.1.1 Tipologie del fascicolo

I fascicoli si dividono in due tipologie:

a) fascicoli relativi ad affari o procedimenti amministrativi
b) fascicoli del personale.

8.1.2 Fascicoli relativi a procedimenti amministrativi

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo.
L'operazione deve essere effettuata dal responsabile dell'ufficio/servizio.
I documenti sono archiviati all'interno di ciascun fascicolo, secondo l'ordine cronologico di registrazione, in base, cioè, al numero di protocollo ad essi attribuito o, se assente, in base alla propria data.
All'inizio del fascicolo è inserito un elenco di tutti i documenti contenuti nello stesso.
Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, il responsabile del procedimento, assegnatario del documento stesso, provvederà all'apertura (istruzione) di un nuovo fascicolo.
Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

8.1.3 Fascicoli del personale

Il fascicolo viene aperto al momento dell'assunzione o riaperto nel caso di ripristino del rapporto di lavoro.
Il fascicolo viene chiuso al momento in cui cessa il rapporto di lavoro.
I fascicoli del personale costituiscono una serie archivistica, da conservare in ordine di categoria (e all'interno della stessa categoria per anzianità di servizio).

8.2 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 sopra citati devono necessariamente seguire le stesse regole che hanno portato alla definizione della struttura e dei campi del titolario di classificazione. Non essendo ancora stati definiti i criteri (omogenei per tutto l'ente) per la definizione dei fascicoli cartacei al momento non sono stati ancora predisposti gli strumenti di reperimento.

8.2.1 Il repertorio dei fascicoli

Attualmente la Camera dispone del repertorio dei fascicoli formati dall'applicazione informatica Prodigi limitatamente agli uffici che hanno effettuato la sperimentazione relativa alla fascicolazione.
L'indice di classificazione di un fascicolo è costituito dai seguenti elementi:

a) anno di apertura
b) classificazione completa (categoria, classe ed eventuale sottoclasse);
c) numero di fascicolo.

Il repertorio dei fascicoli (informatico) è invece costituito dall'indice di classificazione, al quale vanno aggiunti i seguenti elementi:

a) anno di chiusura;
b) oggetto del fascicolo;
c) annotazione dello status relativo all'età: corrente, versato all'archivio di deposito, …;
d) annotazione del passaggio all'archivio storico o, in alternativa, l'avvenuto scarto.

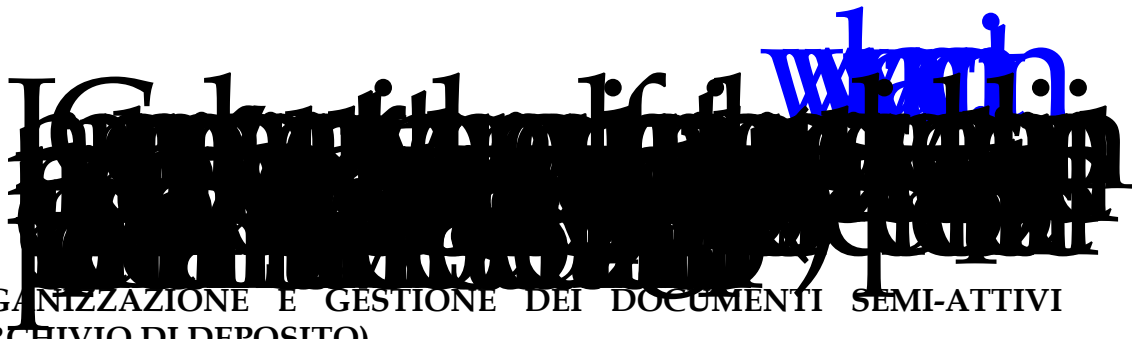
Il repertorio dei fascicoli è un registro annuale, cioè inizia il 1° gennaio e termina il 31 dicembre.

Altri quattro elementi devono garantire la corretta gestione del fascicolo:

a) la data di chiusura;
b) l'annotazione del passaggio dall'archivio corrente all'archivio di deposito;
c) l'annotazione del passaggio dall'archivio di deposito all'archivio storico o, in alternativa l'avvenuto scarto.

8.3 Definizione delle relazioni tra la gestione dei documenti e dei fascicoli e il controllo dei procedimenti amministrativi

La tabella dei procedimenti amministrativi è stata resa pubblica dalla Camera di Commercio di Lucca sul sito internet della Camera all'indirizzo



9 ORGANIZZAZIONE E GESTIONE DEI DOCUMENTI SEMI-ATTIVI (ARCHIVIO DI DEPOSITO)

9.1 Versamento dei fascicoli

Una volta all'anno, ogni ufficio/servizio/dirigente della Camera di Commercio deve trasferire all'archivio di deposito i fascicoli relativi ad affari ed a procedimenti amministrativi conclusi o comunque non più necessari ad una trattazione corrente.

Ogni ufficio/servizio/dirigente predispone un elenco dei fascicoli trasferiti nell'archivio di deposito. Il responsabile del protocollo informatico controlla la corrispondenza tra fascicoli riversati ed elenco presentato e dispone il trasferimento del materiale dall'archivio corrente all'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 sono conservati presso la Segreteria Generale.

L'archivio di deposito della Camera di Commercio di Lucca è costituito dall'archivio di tutti gli atti della Camera compresi gli atti Registro Imprese e Albo Artigiani. Tutti gli archivi sono dislocati in 2 edifici diversi: il primo è adiacente alla Camera, il secondo si trova fuori dal centro storico.

9.2. Movimentazione dei fascicoli

L'affidamento temporaneo di un fascicolo ad una unità organizzativa responsabile o al personale deve avvenire per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.
L'archivio di deposito degli atti, fascicoli della Camera (escluso R.I.) è accessibile a tutti i dipendenti della Camera di Commercio previa richiesta all'ufficio protocollo.
L'archivio di deposito degli atti R.I. è accessibile a tutti, ma è per prassi consultato attraverso il personale R.I..
Non è consentita l'estrazione di documenti in originale dal fascicolo, che vanno anzi tenuti in ordine di sedimentazione rispettando il vincolo archivistico, cioè l'appartenenza di ogni documento alla rispettiva unità archivistica (fascicolo).

9.3 Definizione delle responsabilità delle unità organizzative

Il responsabile del procedimento amministrativo (ad esclusione del R.I.) 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.

10 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.
Almeno ogni 3 anni, la Camera di Commercio di Lucca provvede allo scarto dei documenti relativi a procedimenti conclusi che costituiscono l'archivio di deposito e alla selezione dei documenti relativi agli affari esauriti da oltre 40 anni che devono essere conservati a tempo indeterminato nell'archivio storico dell'Ente la cui gestione e responsabilità è affidata al responsabile del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi.
La Camera di Commercio effettua la selezione attraverso apposita commissione, istituita o modificata con determinazione del Dirigente del Servizio e costituita da:

- il responsabile del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi;
- tre impiegati del Servizio Affari Generali.

Tale commissione deve predisporre un elenco di documenti di cui proporre lo scarto.
Tale elenco deve essere approvato dal Dirigente del Servizio, 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 e di scarto per gli archivi delle Camere di Commercio" relativo al titolario di classificazione utilizzato per l'indicizzazione dei documenti.
Il massimario è stato elaborato da un apposito gruppo di lavoro costituito all'interno del Comitato Tecnico Scientifico degli Archivi delle Camere di Commercio.

La Camera di Commercio di Lucca ha inoltre effettuato 2 riversamenti all'Archivio di Stato dei fascicoli destinati alla conservazione permanente: il primo nel 1861 per i fascicoli del periodo 1366-1848 (questo archivio presenta diverse lacune, solo la parte

relativa al periodo napoleonico è più estesa), il secondo nel 1983 per l'archivio delle Ditte Cessate al 31/12/1942.

11 LA REGISTRAZIONE DEI DOCUMENTI NELL'APPLICAZIONE "PRODIGI"

Il sistema di Protocollo Informatico Prodigi 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 registrazione, le operazioni di segnatura nonché le operazioni di classificazione che costituiscono funzioni necessarie e sufficienti per la sua tenuta.
Il sistema è inoltre predisposto per essere integrato con funzionalità aggiuntive necessarie alla gestione dei flussi documentali, alla conservazione dei documenti ed all'accessibilità alle informazioni.
Nel presente capitolo sono trattati alcuni aspetti dell'applicazione informatica Prodigi: per la descrizione dettagliata delle funzionalità si rimanda al "Manuale Utente Prodigi" .

11.1 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.

11.1.1 Gli elementi obbligatori del protocollo (Registrazione)

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";
b) la data di registrazione assegnata automaticamente dal sistema e registrato in forma "non modificabile", 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.

11.1.2 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.

11.2 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 che sono:

a) dati di registrazione:
   1. data di arrivo (nel formato giorno/mese/anno) solo per le domande R.I.;
   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;
   5. immagine informatica del documento amministrativo in arrivo;

b) dati per la gestione dell'archivio:
   1. classificazione del documento attraverso il titolario (categoria, classe e sottoclasse);
   2. data di istruzione del fascicolo;
   3. numero del fascicolo;
   4. data di chiusura del fascicolo;
   5. repertorio dei fascicoli;
   6. scadenzario;

c) dati per la gestione delle banche dati:
   1. ulteriori informazioni sul mittente (ragione sociale, ecc.);
   2. indirizzo completo del mittente (via, numero civico, c.a.p., città, provincia, stato);
   3. ulteriori informazioni sul destinatario (ragione sociale, ecc.);
   4. indirizzo completo sul destinatario (via, numero civico, c.a.p., città, provincia, stato).

11.3 Annullamento di una registrazione di protocollo

È consentito l'annullamento di una registrazione di protocollo con una specifica funzione riservata al responsabile del Protocollo Informatico e al personale dell'ufficio Protocollo.
L'operazione avviene attraverso l'apposizione 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.

11.4 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.
È consentita la modifica di una informazione registrata in forma non modificabile con una specifica funzione riservata al responsabile del Protocollo Informatico e al personale dell'ufficio Protocollo.

11.5 Segnatura di protocollo

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.
Essa consente di individuare ciascun documento in modo inequivocabile.
Le informazioni minime previste sono:

a- il numero di protocollo, costituito da sette cifre numeriche; tale numerazione si rinnova ad ogni inizio di anno solare;
b- la data di protocollo;
c- l'identificazione in forma sintetica della Camera di Commercio in quanto AOO.

L'operazione di segnatura di protocollo va effettuata contestualmente all'operazione di registrazione di protocollo

L'ufficio Protocollo esegue l'operazione di segnatura per i documenti in arrivo attraverso l'apposizione di un timbro che riporta l'identificazione sintetica della Camera ("Camera di Commercio, Industria e Artigianato LUCCA"), la data di protocollo: i protocollatori completano manualmente i dati variabili (numero di protocollo, categoria e classe).

Per i documenti in partenza i protocollatori provvedono ad inserire manualmente la data e il numero di protocollo negli appositi spazi del documento.

11.6 Registro giornaliero

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

L'ufficio Protocollo provvede alla stampa del giornale con cadenza mensile.

12 SICUREZZA DEL SISTEMA PROTOCOLLO INFORMATICO

12 .1 Definizione dei diritti di accesso e profili utente

Al fine di garantire un corretto accesso ai dati e una corretta ripartizione delle funzioni da rendere disponibili agli utenti sono stati creati appositi profili da associare a ciascun utente che utilizzi il sistema di Protocollo Informatico Prodigi.
Attualmente sono stati definiti per la Camera di Commercio di Lucca i seguenti profili: Protocollatore generale, Protocollatore in uscita, Consultatore e Fascicolatore.

12.1.1. Responsabile del protocollo informatico

Il Responsabile del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi è la persona che oltre ad avere le abilitazioni per le operazioni di protocollazione dei documenti, ha la possibilità di effettuare operazioni di tipo organizzativo e gestionali sul sistema; per esempio:

- predisporre le autorizzazioni di accesso al sistema;
- monitorare le operazione compiute.

Il responsabile del protocollo informatico ha accesso a tutti i dati del protocollo dell'Area Organizzativa Omogenea.
Il responsabile del protocollo esegue controlli a campione sia sulla registrazione dei dati sia sulla congruenza fra il titolario di classificazione e gli strumenti di corredo dell'archivio.
Inoltre il responsabile del protocollo predispone i profili necessari per una corretta ripartizione delle funzioni da rendere disponibili agli utenti.

12.1.2 Protocollatore generale

Il profilo di Protocollatore permette di eseguire la registrazione dei documenti in arrivo/partenza/interni, la segnatura, l'acquisizione dell'immagine del documento mediante uno scanner oppure l'associazione di un file prodotto da un programma informatico.
Consente inoltre di attribuire a tutti i documenti protocollati la classificazione secondo il titolario della Camera e di assegnare il documento in competenza e conoscenza secondo le regole di smistamento descritte nei precedenti capitoli.
Il protocollatore ha infine a disposizione tutti gli strumenti per effettuare la consultazione e la modifica/annullamento di qualsiasi protocollo (secondo quanto descritto nel capitolo 4 e all'art.54 del DPR 28 dicembre 2000, n. 445) e la stampa del registro di protocollo giornaliero.

12.1.3 Protocollatore in uscita

Il profilo di Protocollatore in uscita permette di eseguire la registrazione dei documenti in partenza, la segnatura, l'associazione di un file prodotto da un programma informatico e la scansione dei documenti.
Consente inoltre di attribuire a tutti i documenti protocollati la classificazione secondo il titolario della Camera e di assegnare il documento in competenza e conoscenza secondo le regole di smistamento descritte nei precedenti capitoli.
Ha infine a disposizione tutti gli strumenti per effettuare la consultazione dei protocolli di propria competenza.

12.1.4 Consultatore

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.

L'utente consultatore è abilitato ad accedere al protocollo informatico per la sola consultazione dei documenti . Ha a disposizione principalmente 3 strumenti:

- liste di protocollo dove può consultare i protocolli a lui assegnati in competenza o conoscenza suddivisi in apposite liste
- consultazione dove l'utente inserendo i parametri di ricerca può consultare i documenti ad esso assegnati o assegnati agli uffici/servizi di propria competenza
- liste di controllo dove il responsabile di un'area, servizio o ufficio può consultare i protocolli assegnati al proprio personale suddiviso per area/servizio/ufficio di competenza.

Inoltre ogni consultatore ha la possibilità di inoltrare ad altri i protocolli assegnati (seguendo opportune regole per la competenza/conoscenza) o di rinviare al mittente che ha effettuato lo smistamento se ritiene che il protocollo assegnato non sia di propria competenza.
L'utente consultatore può consultare i fascicoli di propria competenza ed inoltrarli ad altri (secondo le regole per la competenza/conoscenza).

Infine solamente il responsabile del Protocollo Informatico, il personale dell'ufficio Segreteria e Protocollo hanno la visibilità su tutti documenti registrati (ad eccezione di quelli riservati).

12.1.5 Fascicolatore

L'utente fascicolatore ha la possibilità di creare e gestire i propri fascicoli. Può inserire nei propri fascicoli i documenti protocollati ad esso assegnati in competenza (o assegnati ad uffici/servizi di propria pertinenza), inoltrare i propri fascicoli ad altri uffici/servizi (in competenza o conoscenza), effettuare le operazioni di ricerca e consultazione (limitatamente ai fascicoli di propria competenza) e chiudere i propri fascicoli nel caso il procedimento sia esaurito.

12 .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 dovranno essere inserite nel protocollo informatico. 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.

13 INTEROPERABILITA': DESCRIZIONE DEI LIVELLI DI ATTIVAZIONE DELLE FUNZIONI DI INTEROPERABILITA'

La ricezione e la trasmissione dei documenti informatici che assicurino il rispetto della normativa vigente è assicurata tramite una casella di posta istituzionale riservata a questa funzione ed accessibile solo al personale preposto alla loro registrazione di protocollo e alla loro gestione.

Il sistema informatico di gestione protocollo "Prodigi" consente l'interoperabilità tra la Camera di Commercio e le altre amministrazioni: la Camera di Commercio di Lucca non ha ancora sperimentato l'interoperabilità.

14 ACCESSO E PROTEZIONE DEI DATI

14.1 Organizzazione

La Camera di Commercio è costituita da UOC in rappresentanza del Segretario Generale e dei dirigenti di uno o più servizi.
Oltre a personale in staff ci possono essere uffici organizzati orizzontalmente che dipendono dalla stessa UOC.

14.2 Visibilità dei protocolli

Con visibilità di un protocollo si intende la possibilità di consultare le proprietà del documento (cioè i dati istituzionali e i dati gestionali registrati in archivio), il suo contenuto cioè i documenti allegati (sia scannerizzati che informatici) e tutte le operazioni fatte sul protocollo (tracciatura delle operazioni e modifiche).

- I protocolli devono essere visibili dalla user che li ha inseriti, dalle user con pari abilitazioni (cioè tutte quelle dello stesso ufficio protocollo) e dal responsabile di protocollo.
- La visibilità dei protocolli deve essere piramidale: ogni UOC 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 e quelli degli addetti nell'ambito dello stesso ufficio.
- Se una UOC ha sotto di sé servizi o uffici o persone che rispondono gerarchicamente ad un'altra UOC, 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.

14.3 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 o richiesto dall'Ufficio, se trattasi di documento riservato.
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.

Sulla stampa del registro giornaliero comparirà solo il nr. e la data di protocollazione con la dicitura protocollo riservato.

14.4 Modifica dei protocolli

L'ufficio Protocollo e il Responsabile del protocollo possono accedere a tutti i protocolli per le modifiche (eccetto quelli riservati).
Il personale abilitato alla protocollazione in uscita può modificare solo i protocolli di propria competenza.
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.

15 DISPOSIZIONI FINALI

15.1 Modalità di adozione degli aggiornamenti al manuale

Il Segretario Generale, in qualità di Responsabile del servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi propone alla Giunta l'adozione delle modifiche al Manuale di Gestione.
Gli aggiornamenti possono riguardare anche solo una sezione o allegato del Manuale.
Gli aggiornamenti sono previsti nei seguenti casi:

1. revisione del Titolario di classificazione;
2. revisione del Massimario di selezione;
3. variazioni sostanziali alle procedure informatiche di gestione del protocollo;
4. modificazioni agli assetti organizzativi della Camera di Commercio che incidono sulle procedure descritte nel manuale;

15.2 Modalità di comunicazione del manuale

Il Manuale viene pubblicato nella sezione "atti on-line" del sito internet della Camera e all'Albo della Camera di Commercio, sulla intranet camerale previa adeguata comunicazione al personale e sul sito internet della Camera.

15.3 Ulteriori riferimenti

Per quanto non espressamente previsto dal presente manuale, si fa riferimento alla normativa vigente in materia, adottando comportamenti ispirati al principio del buon andamento dell'attività amministrativa.

Allegati

In allegato al presente manuale si trovano i seguenti documenti:

1. organigramma
2. titolario di classificazione
3. massimario