MANUALE PER LA GESTIONE DEL PROTOCOLLO INFORMATICO,

DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

SEZIONE I – IL MANUALE DI GESTIONE

1.1 AMBITO DI APPLICAZIONE

Il presente "Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi" (d'ora in poi Manuale di Gestione) - adottato ai sensi dell'art. 5 del DPCM 2 dicembre 2013 ("Regole tecniche per il protocollo informatico ai sensi degli articoli n.40 bis, 41, 47, 57 bis e 71 del Codice dell'Amministrazione digitale di cui al decreto legislativo n.82 del 2005") disciplina le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti della Camera di commercio industria artigianato e agricoltura di Genova.

1.2 AREA ORGANIZZATIVA OMOGENEA (AOO)

Ai fini della gestione documentale, la Camera di commercio di Genova individua un'unica Area Organizzativa Omogenea (AOO), composta dall'insieme di tutti gli Uffici (Unità Organizzative Responsabili UOR), come rappresentato nell'organigramma allegato al presente Manuale (v. allegato n.1), in quanto tutti gli Uffici presentano esigenze di gestione unica e coordinata dei documenti, con criteri uniformi di classificazione e archiviazione (v. art.50, comma 4 del DPR 28 dicembre 2000, n.445). Con delibera n.8 del 2004 si è provveduto a individuare nell'ambito dell'Area Organizzativa Omogenea il Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi di cui all'art. 61 del DPR n.445/2000.

1.3 INDIVIDUAZIONE DEGLI UFFICI CHE OPERANO LA REGISTRAZIONE DI PROTOCOLLO

La Camera di Commercio di Genova adotta un modello organizzativo parzialmente decentrato per quanto riguarda la protocollazione dei documenti in arrivo e in partenza.
I documenti in arrivo vengono registrati nel Protocollo generale presso le postazioni abilitate presenti nell'Ufficio Affari Generali e Protocollo sito nella sede camerale di Via Garibaldi 4. Nel caso di documenti cartacei, per velocizzarne i tempi di protocollazione è stata attribuito il profilo di protocollatore dei documenti in entrata anche ad alcuni addetti che operano nelle sedi distaccate: presso l'Ufficio Registro Imprese, l'Ufficio Artigianato e l'Ufficio Abilitazioni speciali, siti in P.zza De Ferrari 2, e presso gli Uffici della sede di Chiavari (c.so Genova 24).

La protocollazione delle lettere in uscita è stata invece interamente decentrata a partire dal 6 marzo 2017, giorno in cui è entrato in funzione il sistema di Gestione Documentale "GEDOC", fornito da Infocamere S.c.p.A.: di conseguenza, in ogni Ufficio camerale sono presenti uno o più operatori a cui è stato attribuito il profilo che consente la protocollazione e la spedizione di un documento in uscita.

SEZIONE II - LE TIPOLOGIE DOCUMENTALI E I FLUSSI DOCUMENTALI

2.1 IL DOCUMENTO AMMINISTRATIVO

Per documento amministrativo viene intesa "ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa" (art.1, lett. a) DPR 445/2000). In riferimento al tipo di supporto i documenti amministrativi gestiti dalla Camera di Commercio di Genova possono essere distinti in informatici o analogici.

2.1.1 IL DOCUMENTO INFORMATICO

L'art.40 del Codice dell'Amministrazione digitale (D.Lgs. 7 marzo 2005, n.82) stabilisce che "le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici". In accordo con quanto previsto dalle "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici" (DPCM 13 novembre 2014), il documento informatico è formato mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi strumenti software;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

La copia analogica di un documento informatico consiste nella copia, di norma cartacea, di un documento amministrativo prodotto in origine su supporto informatico.

La firma digitale - equivalente elettronico della tradizionale firma autografa su carta - è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità, la non ripudiabilità. E' basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

2.1.2 IL DOCUMENTO ANALOGICO

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

La copia informatica di un documento analogico consiste nella copia del documento amministrativo prodotta su supporto informatico (es. il file immagine risultante dalla scansione del documento cartaceo).

Dal 6 marzo 2017, cioè da quando è in uso il sistema di gestione documentale GEDOC, i documenti in uscita della Camera di Commercio di Genova sono esclusivamente documenti informatici. Se il destinatario non ha fornito un indirizzo di posta elettronica a cui recapitare il documento, o tale indirizzo non risulta funzionante, viene prodotta una copia analogica per la spedizione via posta ordinaria o raccomandata: in tale eventualità (come viene riportato sul modello utilizzato per redigere le lettere in uscita) il documento stampato su supporto cartaceo costituisce una copia analogica dell'originale informatico, predisposto e conservato dalla Camera di Commercio in conformità alle regole tecniche di cui al D.P.C.M. 13 novembre 2014.

2.2 REGIME GIURIDICO DEI DOCUMENTI DELLA CAMERA DI COMMERCIO

A norma dell'art. 10, c. 2 lett. b), e dell'art. 21 del D. Lgs. 22/1/2004 n. 42 (Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137) tutti i documenti della Camera di Commercio dal momento del loro inserimento nell'archivio camerale mediante l'attribuzione di un codice di classificazione in quanto beni culturali sono sottoposti a particolari tutele e garanzie: ai sensi dell'art. 21, c.2, del D.Lgs. 42/2004 è necessario chiedere l'autorizzazione della Soprintendenza archivistica per lo spostamento di fondi dell'archivio di deposito e dell'archivio storico, e per lo scarto di documentazione archivistica; inoltre, qualora abusivamente sottratti alla Camera di Commercio, i documenti del suo archivio sono rivendicabili senza limiti di tempo, purché si disponga di elementi che ne provino l'appartenenza (carta intestata, numeri di protocollo, indici di classificazione, descrizioni di inventari, etc.).

2.3 DOCUMENTI PER I QUALI NON È PREVISTA LA REGISTRAZIONE

Tutti i documenti ricevuti e spediti dalla Camera di Commercio di Genova sono sottoposti a registrazione di protocollo, con esclusione di alcune tipologie di documenti già sottoposti a registrazione particolare (*v. infra cap.2.7*) e dei documenti per i quali non è obbligatoria la registrazione di protocollo.

In particolare, i documenti, siano essi informatici o analogici, per i quali la Camera di Commercio non prevede la registrazione di protocollo sono:

a) gazzette ufficiali;

b) bollettini ufficiali;

c) notiziari della pubblica amministrazione;

d) materiali statistici;

e) atti preparatori interni;

f) giornali e riviste;

g) libri;

h) opuscoli e pubblicazioni varie;

i) depliant;

j) materiali pubblicitari;

k) inviti a manifestazioni che non danno adito all'attivazione di un procedimento amministrativo;

l) documenti di occasione aventi carattere effimero (ringraziamenti, richieste di appuntamenti con i dirigenti, congratulazioni varie, condoglianze);

m) qualunque tipo di comunicazione avente carattere esclusivamente informativo, quali documenti e report interni (ordini di trasferta, note spese, reportistica, modulistica del personale ecc.), modelli fiscali;

n) le ricevute di accettazione, consegna e mancata consegna pervenute a seguito di una spedizione via pec

o) documenti anonimi (v. *infra cap.3.8)*

2.4 DOCUMENTI IN ENTRATA

Per documenti in entrata si intendono tutti i documenti pervenuti alla Camera di Commercio tramite:

- Posta elettronica (ordinaria e PEC)
- pratiche telematiche
- servizio postale tradizionale (posta ordinaria, prioritaria, raccomandata, ecc.), consegna tramite corriere e notifica (postale o a mano)
- consegna diretta
- telefax

2.4.1 POSTA ELETTRONICA (ORDINARIA E CERTIFICATA)

In virtù di quanto stabilito dal D.P.R. 11/2/2005 n. 68 ("Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata"), e dal D.Lgs. 7/3/2005 n.82 e s.m.i. (Codice dell'Amministrazione digitale), la Camera di Commercio di Genova si è dotata di una casella di posta elettronica certificata (PEC) istituzionale: cciaa.genova@ge.legalmail.camcom.it, indicata nella home page del sito internet istituzionale e nell'IPA (l'Indice delle Pubbliche Amministrazioni realizzato e gestito dall'Agenzia per l'Italia digitale). La casella PEC è di tipo cd. "aperto", cioè può ricevere messaggi provenienti anche da caselle di posta elettronica ordinaria, ed è gestita dall'Ufficio Affari Generali – Protocollo, che ne garantisce il monitoraggio costante nell'arco della giornata lavorativa.

Nel caso in cui venga ricevuto un messaggio di posta elettronica nella casella di posta elettronica certificata istituzionale sopra indicata, esso è immediatamente protocollato, utilizzando le funzionalità messe a disposizione dal sistema di gestione documentale (la casella PEC infatti è

collegata al sistema GEDOC – v. paragrafo n.4.1). Fanno eccezione i casi di cui al paragrafo 2.3: l'addetto alla protocollazione valuta caso per caso se si tratta di un documento che può essere comunque inoltrato tramite GEDOC ma senza protocollazione oppure se può essere eliminato (nel caso ad es. di materiale pubblicitario).

Nel caso in cui il messaggio di posta elettronica (ordinaria o certificata) pervenga ad una casella di posta elettronica diversa da quella istituzionale sopra indicata, esso dovrà essere trasmesso senza indugio, a cura dell'utente che lo ha ricevuto, alla casella di posta elettronica dell'Ufficio Protocollo, che provvederà a protocollare il documento inserendolo nel sistema GEDOC.

Nel caso in cui il documento venga successivamente ricevuto anche per via ordinaria, dovrà essere rispettata la seguente procedura:

a) Nel caso in cui il documento pervenuto per via ordinaria sia assolutamente identico al documento anticipato via posta elettronica, l'operatore di protocollo riporterà sul documento pervenuto per via ordinaria i dati di registrazione del documento anticipato via posta elettronica, inserendo nel campo "note" della registrazione di protocollo la menzione della duplice modalità di trasmissione;

b) Nel caso in cui l'operatore di protocollo riscontri qualche correzione o modifica, anche minima, nel documento pervenuto per via ordinaria rispetto al documento anticipato via posta elettronica, o non sia possibile accertarsi dell'identità tra i due documenti, dovrà effettuare una nuova registrazione di protocollo.

2.4.2 PRATICHE TELEMATICHE

La Camera utilizza questo canale di ricezione per la fatturazione elettronica (attiva e passiva) e per tutte le domande di iscrizione, modifica e cancellazione al Registro Imprese, nonché per tutte le denunce del REA – Repertorio delle notizie economico amministrative e la relativa documentazione allegata. Tramite invio telematico sono presentate anche le domande di rilascio/convalida del codice meccanografico - Sistema ITALIANCOM (Italian Companies Around the World), le domande di iscrizione al Registro Telematico Gas fluorurati, al Registro Produttori apparecchiature elettriche ed elettroniche (R.A.E.E.), al Registro Pile e accumulatori e al M.U.D. (modello unico di dichiarazione ambientale). Il canale telematico è utilizzato anche per le domande relative ai titoli della proprietà industriale (brevetti per invenzione e modelli di utilità, marchi, disegni).

2.4.3 SERVIZIO POSTALE E CONSEGNA DIRETTA O TRAMITE CORRIERE O NOTIFICA

La corrispondenza indirizzata alla sede della Camera di Commercio viene consegnata al personale ausiliario della Camera di Commercio di norma nell'arco della mattinata. La corrispondenza così raccolta viene consegnata all'Ufficio Protocollo. Nel caso in cui la corrispondenza venga consegnata manualmente ad uffici della sede, diversi dall'Ufficio Protocollo, essa deve essere tempestivamente inoltrata all'Ufficio Protocollo.

Il personale dell'Ufficio Protocollo provvede senza indugio, e comunque nell'arco della giornata, all'apertura della posta. Le buste relative alla corrispondenza ordinaria vengono conservate presso l'Ufficio Protocollo per 3 mesi. Quelle della posta pervenuta per raccomandata vengono conservate per 6 mesi, a meno che l'Ufficio destinatario della pratica non richieda espressamente che la busta venga allegata al documento protocollato.

La corrispondenza non viene aperta nel caso in cui si evinca il carattere personale o riservato (ad es. posta indirizzata a un nominativo specifico "c/o CCIAAA" o espressioni similari, oppure riportante indicazione "riservata", "personale", "confidenziale" e simili): in questi casi la corrispondenza viene consegnata direttamente al destinatario, il quale, dopo averne preso visione, se valuta che i documenti ricevuti non sono personali, è tenuto a trasmetterli all'ufficio protocollo per la protocollazione.

Anche la corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili, o comunque dalla cui busta si evinca la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo e della data di registrazione direttamente sulla busta (plico o simili). Se la scadenza relativa alla gara, bando o concorso cade nel giorno in cui viene effettuata la protocollazione, e la busta viene consegnata a mano presso l'Ufficio Protocollo, accanto al timbro di protocollo l'operatore indica anche l'ora di consegna effettiva.

2.4.4 TELEFAX

L'uso del fax soddisfa il requisito della forma scritta e quindi, non è necessario che sia seguito dalla trasmissione del documento originale (art. 38 c.1 e 43 c.6 del DPR 445/2000).

Il documento in arrivo trasmesso via fax deve essere registrato nel sistema di protocollo informatico della Camera di Commercio insieme alla copertina di trasmissione, se presente. Qualora il documento venga successivamente ricevuto anche per via ordinaria, dovrà essere rispettata la seguente procedura:

a) Nel caso in cui il documento pervenuto per via ordinaria sia assolutamente identico al documento anticipato via fax, l'operatore di protocollo riporterà sul documento pervenuto per via ordinaria i dati di registrazione del documento anticipato via fax, inserendo nel campo "note" della registrazione di protocollo la menzione della duplice modalità di trasmissione;

b) Nel caso in cui l'operatore di protocollo riscontri qualche correzione o modifica, anche minima, nel documento pervenuto per via ordinaria rispetto al documento anticipato via fax, o non sia possibile accertarsi dell'identità fra i due documenti, dovrà effettuare una nuova registrazione di protocollo.

2.5 DOCUMENTI IN USCITA

Per documenti in uscita si intendono i documenti prodotti nell'esercizio delle proprie funzioni dal personale in servizio presso la Camera di Commercio e indirizzati a destinatari esterni all'Ente.

I documenti in uscita devono riportare le seguenti informazioni:

a) logo della Camera di Commercio e dicitura “Camera di Commercio, Industria, Artigianato e Agricoltura di Genova“;

b) indirizzo completo della Camera di Commercio (via, numero, c.a.p., città, provincia);

c) numero di telefono e fax della Camera di Commercio;

d) indirizzo di posta elettronica della Camera di Commercio;

e) luogo e data completa (giorno, mese, anno);

g) oggetto del documento;

h) numero degli allegati al documento;

i) indicazione del RPA (Responsabile del procedimento amministrativo) o del Dirigente.

I documenti in uscita sono redatti sulla base di modelli predisposti in formato “.docx” e scaricabili da una sezione dedicata della rete intranet. Le bozze di documento in uscita sono poi convertite automaticamente dal sistema GEDOC in file di formato “pdf/A”, che vengono successivamente perfezionati con l’apposizione della firma digitale (in modalità cd. “PADES”) ai sensi dell’art.24 del D.Lgs. 82/2005 e con l’apposizione dei dati relativi alla registrazione di protocollo.

2.5.1 TRASMISSIONE DEI DOCUMENTI IN USCITA

I documenti in uscita sono formati come documenti informatici e spediti via PEC utilizzando il sistema di Gestione Documentale GEDOC: la protocollazione e la spedizione sono quindi sempre decentrate. Quando però la spedizione via PEC non è possibile (ad esempio nel caso in cui il destinatario abbia un indirizzo email non funzionante), la fase di spedizione diventa di competenza dell’Ufficio Posta: l’Ufficio che cura la pratica provvede a creare una copia analogica dell’originale informatico, e ad inviarla per la spedizione all’Ufficio Posta.

Nel caso di spedizione informatica, GEDOC associa automaticamente alla registrazione di protocollo la ricevuta di accettazione (in caso di spedizione a email ordinarie o PEC) e la ricevuta di consegna (in caso di spedizione a PEC). Le ricevute di mancata consegna vengono invece gestite dall’Ufficio Protocollo, che provvede ad inoltrarle all’Ufficio interessato. In ogni caso, l’addetto che ha effettuato la spedizione di un documento in uscita ha sempre l’onere di verificare, accedendo a GEDOC, il buon esito della spedizione, controllando se è presente o meno la ricevuta di avvenuta consegna.

2.6 DOCUMENTI INTERNI

Per documenti interni si intendono i documenti scambiati tra differenti Uffici, Servizi o Aree della Camera di Commercio. I documenti interni di preminente carattere informativo, quali memorie informali, appunti, brevi comunicazioni non vengono registrati. Gli ordini di servizio vengono sottoposti a registrazione particolare (cfr. 2.7.10).

Sono, invece, registrati nel sistema di Gestione Documentale della Camera di Commercio i documenti interni di preminente carattere giuridico - probatorio, redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità dell'azione amministrativa, e qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Il sistema GEDOC consente di fascicolare e successivamente inviare in conservazione qualsiasi documento informatico, anche senza procedere alla registrazione di protocollo: ogni operazione viene in ogni caso tracciata secondo la normativa vigente.

2.7 INDIVIDUAZIONE DI TIPOLOGIE PARTICOLARI DI DOCUMENTI PER I QUALI SI STABILISCONO MODALITÀ DI REGISTRAZIONE PARTICOLARE

Esistono tipologie di documenti che, per disposizioni normative, regolamentari o semplicemente organizzative, sono soggetti a forme di trattamento e registrazione particolare. Tali documenti possono essere sottoposti a registrazione particolare (cfr. art. 53, comma 5 del DPR 445/2000). Con cadenza annuale verranno effettuate opportune verifiche per l'adozione di misure organizzative e tecniche per l'eventuale eliminazione dei protocolli di settore e di reparto, e più in generale dei protocolli diversi dal protocollo informatico ancora presenti nella AOO.

Di seguito si riportano le tipologie di documento che la Camera di Commercio tratta con modalità di registrazione particolare (l'insieme minimo dei metadati associati ai documenti è riportato nell'Allegato n.4):

2.7.1 DELIBERE E DETERMINAZIONI

Le delibere e le determinazioni, in quanto documenti già soggetti a registrazione particolare da parte dell'Amministrazione, non sono registrati nel sistema di protocollo informatico della Camera di Commercio.

2.7.1.1 Serie delle delibere e delle determinazioni e rispettivo repertorio generale

Le delibere adottate e le comunicazioni effettuate in una riunione (di Giunta o Consiglio) vengono raccolte e rilegate in un unico verbale della riunione, al quale si attribuisce un numero progressivo con cadenza annuale.

Ciascun complesso delle delibere e determinazioni dirigenziali costituisce una serie. Ciascuna serie delle delibere e delle determinazioni deve essere corredata da un proprio repertorio generale, ossia un numero progressivo che ha cadenza annuale, cioè inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Per consuetudine interna, accanto al numero della determinazione è apposta una lettera per indicare la presenza (lettera "B") o meno (lettera "Z") dell'impegno di spesa, oppure per indicare che trattasi di atto riguardante il personale (lettera "A").

Sono rilegate in serie annuali:

a) Le delibere della Giunta Camerale e le comunicazioni del Presidente alla Giunta camerale;

b) Le delibere del Consiglio Camerale;

c) Le determinazioni d'urgenza del Presidente;

d) Le determinazioni del Segretario Generale e dei Dirigenti.

2.7.1.2 Gestione e archiviazione delle delibere e delle determinazioni

Ogni proposta di delibera e determinazione deve essere inserita nell'applicativo denominato "Legal Work Act", per la gestione dematerializzata degli atti. Il Sistema Legal Work Act permette la completa gestione dei flussi deliberativi e determinativi, dalla nascita di una proposta alla trasformazione della stessa in delibera o determinazione attraverso tutti i passaggi intermedi. Il Sistema LWA è integrato al sistema per la conservazione presente in GEDOC (v. paragrafo n. 6.5), e permette quindi di correlare la fase di deliberazione alla fase di archiviazione e conservazione dei documenti. Viene comunque conservata presso l'Ufficio Affari Generali e Protocollo una copia cartacea di ogni atto (determinazione e delibera). Dopo l'approvazione dei verbali di Giunta, delle relative delibere viene redatta copia conforme all'originale e inviata all'Ufficio proponente.

2.7.1.3 Pubblicazione delle delibere all'albo on line

A partire dal 1 gennaio 2011, gli obblighi di pubblicazione di atti e provvedimenti amministrativi delle amministrazioni e degli enti pubblici che hanno effetto di pubblicità legale, si intendono assolti con la pubblicazione degli stessi nei rispettivi siti informatici. Per questo motivo la Camera di Commercio di Genova ha inserito nella home page del proprio sito internet istituzionale un collegamento alla pagina dell'Albo on line, dove deliberazioni e altri atti e documenti sono consultabili per tutta la durata del periodo di pubblicazione (7 giorni per le deliberazioni, come previsto dall'art.62 del R.D. n .2011/1934). Decorso il periodo di pubblicazione, è possibile consultare i provvedimenti pubblicati facendo richiesta di accesso con le modalità previste dalla legge n.241/1990.

La Camera di Commercio ha provveduto anche ad adottare un Regolamento per la tenuta dell'Albo camerale on line (approvato con deliberazione del Consiglio camerale n.9/C del 18 luglio 2011).

2.7.2 DENUNCE AL REGISTRO DELLE IMPRESE

Le denunce di iscrizione, modifica o cancellazione al Registro delle Imprese, sia quelle inviate per posta ordinaria che quelle inoltrate per via telematica nonché le domande di vidimazione dei libri sociali sono soggette a registrazione particolare da parte dell'Ufficio Registro Imprese e, pertanto, non vengono registrate nel sistema di protocollo informatico della Camera di Commercio.

Tutte le altre tipologie di documento gestite dall'Ufficio Registro Imprese, quali, solo a titolo esemplificativo, le richieste di accertamento inviate a coloro che hanno presentato le domande, l'invio dei suddetti accertamenti da parte dei diretti interessati, e le richieste di

visure/certificati/elenchi pervenute via posta, non sono soggette a registrazione particolare da parte dell'Ufficio Registro Imprese e, pertanto, vengono registrate nel sistema di protocollo informatico della Camera di Commercio.

I certificati, visure ed elenchi rilasciati agli sportelli dell'Ufficio Registro Imprese, non sono sottoposti a registrazione da parte della Camera di Commercio.

2.7.3 PROTESTI CAMBIARI

I seguenti atti, inviati alla Camera di Commercio, o consegnati a mano all'Ufficio Protesti, sono soggetti a registrazione particolare da parte dell'Ufficio stesso e, pertanto, non vengono registrati nel sistema di protocollo informatico della Camera di Commercio:

• gli elenchi inviati all'Ufficio Protesti dagli Ufficiali Levatori

• i decreti di riabilitazione

• le richieste di annotazione sugli effetti cambiari

• le istanze di cancellazione dal registro protesti

Sono soggetti a registrazione nel sistema di protocollo informatico della Camera di Commercio tutte le altre tipologie di documenti quali ad esempio:

• i ricorsi in materia di Protesti Cambiari, ex art. 700 C.p.C. notificati alla Camera di Commercio dal Tribunale competente;

• le lettere, inviate ai diretti interessati e relative all'esito dell'istanza di cancellazione presentata presso l'Ufficio Protesti;

• le rettifiche o comunicazioni eventualmente presentate dagli Ufficiali Levatori di qualsiasi genere e natura attinenti alla materia.

2.7.4 DOMANDE DELLA CARTA DEL CONDUCENTE

La carta tachigrafica è il dispositivo che consente l'utilizzo dell'unità veicolare (tachigrafo) nelle sue diverse funzioni. Permette, innanzitutto, di identificare il soggetto che opera con il tachigrafo, sia esso un conducente, un'autorità di controllo, un'officina di manutenzione o un'azienda proprietaria del veicolo. Le domande di Carta Tachigrafica del Conducente, dell'Officina, dell'Azienda e di Controllo vengono trasmesse direttamente all'Ufficio Servizi Innovativi e sono soggette a registrazione particolare.

2.7.5 DOMANDE DI BREVETTI E MARCHI

Le domande relative a marchi o brevetti, i seguiti, le istanze, le tasse, l'invio telematico di domande di brevetti al Ministero competente sono soggette a registrazione particolare da parte dell'Ufficio Brevetti e, pertanto, non vengono registrate nel sistema di protocollo informatico della Camera di Commercio.

Le lettere di trasmissione delle domande al Ministero, le relative risposte e la comunicazione al diretto interessato dell'avvenuto rilascio o meno del brevetto vengono registrate nel sistema di protocollo informatico della Camera di Commercio.

2.7.6 ALBO NAZIONALE GESTORI AMBIENTALI

Tutta la corrispondenza indirizzata all'Albo Nazionale Gestori Ambientali (sezione regionale della Liguria), che ha sede presso la Camera di Commercio di Genova (P.zza De Ferrari 2), viene inoltrata (senza essere aperta) direttamente agli uffici competenti.

2.7.7 RICHIESTE DI CERTIFICATI DI ORIGINE E CARNET ATA

I moduli di richiesta di Certificati di Origine e Carnet ATA sono soggetti a registrazione particolare da parte dell'Ufficio Commercio Estero, e non vengono quindi registrati nel sistema di protocollo informatico della Camera di Commercio.

2.7.8 REGISTRAZIONI DI CONTABILITÀ E BUONI D'ORDINE

I mandati e le reversali sono soggetti a registrazione particolare da parte dell'Ufficio Ragioneria e, pertanto, non vengono registrati nel sistema di protocollo informatico della Camera di Commercio.

I buoni d'ordine per acquisto di beni o servizi, sia in forma cartacea che telematica (sul portale degli acquisti della Pubblica Amministrazione, www.acquistinretepa.it) sono soggetti a registrazione particolare da parte dell'Ufficio Provveditorato.

2.7.9 PROTOCOLLI RISERVATI

Qualsiasi tipo di comunicazione riservata è gestita tramite il sistema di protocollo informatico, attribuendo il carattere di "RISERVATO" alla registrazione di protocollo. La possibilità di registrare protocolli riservati è attribuita solo agli operatori dell'Ufficio Protocollo. La registrazione così effettuata è visibile solo da parte dell'utente cui è stato assegnato il protocollo. I metadati associati al documento registrato come riservato sono gli stessi attribuiti alle altre registrazioni di protocollo effettuate tramite il sistema di Gestione documentale GEDOC (v. paragrafo n.4.1).

2.7.10 ORDINI DI SERVIZIO

Gli ordini di servizio emessi dal Segretario Generale sono numerati progressivamente e ordinatamente conservati in apposita raccolta e, pertanto, non vengono registrati nel sistema di protocollo informatico della Camera di Commercio**.**

SEZIONE III – LA REGISTRAZIONE DI PROTOCOLLO

3.1 REGISTRAZIONE DEI DOCUMENTI

Il registro di protocollo è un atto pubblico che fa fede della data di ricevimento o spedizione di un documento (indipendentemente dalla regolarità del documento stesso) ed è idoneo a produrre effetti giuridici. La registrazione di protocollo è un atto pubblico di fede privilegiata: attesta cioè, fino a querela di falso, l'avvenuta ricezione/trasmissione di un documento e la data di tale evento.

Il registro di protocollo è gestito mediante il sistema di Gestione Documentale GEDOC fornito da Infocamere ScpA. Nell'ambito della AOO il registro di protocollo è unico, e unica è la numerazione progressiva delle registrazioni di protocollo: la numerazione si chiude il 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

3.2 ORDINE DI PRIORITÀ NELLA REGISTRAZIONE E PROTOCOLLO DIFFERITO

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata. Le raccomandate (in entrata e in uscita), gli atti notificati, le PEC sono protocollati con precedenza sugli altri documenti, salvo diverse indicazioni provenienti dagli Uffici camerali. In presenza di eccezionali quantitativi di documenti da protocollare, gli addetti dell'Ufficio Protocollo provvedono a rispettare l'ordine di arrivo dei vari documenti (anche utilizzando il timbro riportante la data di arrivo al Protocollo - v. Allegato n.2), mantenendo ferme le priorità di cui sopra.

Eccezionalmente qualora dalla mancata registrazione a protocollo di un documento in arrivo, nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi (gare, concorsi e simili), verranno differiti i termini di registrazione del documento, con apposito provvedimento del Responsabile della Gestione Documentale. Nel provvedimento di differimento verranno specificati: le cause del differimento, i documenti da ammettere alla registrazione differita e i termini entro il quale la registrazione di protocollo dovrà comunque essere effettuata. Su ciascun documento ammesso al differimento della registrazione di protocollo, dovrà comunque essere apposto il timbro di arrivo.

Per evitare ritardi e garantire una più efficiente gestione delle procedure relative allo svolgimento di gare, concorsi e simili, gli Uffici camerali interessati dovranno tempestivamente comunicare all'Ufficio Protocollo, con un congruo anticipo, l'indizione e la scadenza di gare, offerte, concorsi e simili.

3.3 REGISTRAZIONE DEI DOCUMENTI IN ARRIVO

La registrazione di un documento in arrivo avviene attraverso la memorizzazione, nel sistema di Gestione Documentale GEDOC della Camera di Commercio, dei seguenti elementi:

a) data di registrazione (assegnata automaticamente dal sistema);

b) numero di protocollo (assegnato automaticamente dal sistema)

c) data di arrivo;

d) data e numero del protocollo del documento in arrivo (se disponibili);

e) mittente;

f) oggetto;

g) numero ed, eventualmente, descrizione degli allegati;

h) indice di classificazione del documento;

i) modalità di ricezione;

j) impronta digitale del documento (per i documenti informatici);

k) assegnatario in competenza del documento

Per la corrispondenza che riporti esplicitamente la dicitura “gara”, “concorso” e simili, o dalla cui busta sia comunque deducibile la partecipazione ad una gara, concorso, ecc. vengono registrati solo gli elementi disponibili rilevabili dalla busta chiusa.

Qualora venga erroneamente registrato un documento di competenza di terzi (altro ente, altra persona fisica o giuridica), la registrazione va annullata (cfr. 3.8, lett. c).

3.4 SEGNATURA DEI DOCUMENTI IN ENTRATA

La segnatura di un documento in entrata viene effettuata direttamente dal sistema di gestione documentale con l’apposizione dei dati di registrazione di protocollo sul file pdf, nel caso di documenti scansionati. In tutti gli altri casi, la segnatura è costituita da un file che viene associato alla registrazione di protocollo ai sensi della normativa vigente.

Nel caso in cui il documento in arrivo sia cartaceo, l’originale cartaceo viene comunque trasmesso all’Ufficio competente, previa apposizione del timbro di protocollo, con le seguenti informazioni:

a) nome identificativo dell’amministrazione (Camera di Commercio di Genova);

b) numero di protocollo;

c) data di protocollo;

d) indice di classificazione del documento, suddiviso in categoria, classe ed eventuale sottoclasse (CAT – CLASSE – FASC).

Per la corrispondenza che riporti esplicitamente la dicitura “gara”, “concorso” e simili, o dalla cui confezione sia comunque deducibile la partecipazione ad una gara, concorso, ecc. la segnatura di protocollo verrà apposta direttamente sulla busta, plico o simili. Se la protocollazione viene effettuata nella giornata in cui cade il termine di presentazione delle domande di partecipazione, il protocollista apporrà anche l’indicazione dell’ora di arrivo (se la busta viene consegnata direttamente all’Ufficio Protocollo).

3.5 SCANSIONE DEI DOCUMENTI

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura protocollo, sono acquisiti in formato ".pdf" mediante il processo di scansione. Non si procede a scansione qualora il documento sia costituito da un numero di pagine tale da rendere troppo elevate le dimensioni del file risultante per i parametri di GEDOC (i file di dimensioni superiori a 30 Mb infatti non possono essere associati alla registrazione di protocollo).

Il processo di scansione si articola nelle seguenti fasi:

• acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un file in un formato standard abilitato alla conservazione (formato .pdf);

• verifica della leggibilità, accessibilità e qualità dei file acquisiti;

• collegamento dei file alle rispettive registrazioni di protocollo, in modo non modificabile.

3.6 SMISTAMENTO E ASSEGNAZIONE DEI DOCUMENTI IN ARRIVO

L'attività di smistamento consiste nell'operazione di inviare un documento protocollato e segnato all'Ufficio competente: con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione. L'assegnazione può essere effettuata per conoscenza o per competenza. L'Ufficio competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

I documenti ricevuti dall'Ufficio Protocollo, dopo essere stati registrati e classificati, vengono smistati all'Unità Organizzativa responsabile, individuata in base alle indicazioni fornite dal Segretario_Generale oppure al modello delle competenze definito dall'organigramma. I documenti informatici vengono smistati all'Ufficio competente tramite il sistema di Gestione documentale GEDOC, quelli analogici anche tramite inoltro via posta interna.

In caso di dubbio riguardo all'assegnazione del documento protocollato, in particolar modo di fronte a nuove tipologie documentali, l'Ufficio Protocollo chiede chiarimenti all'Ufficio competente per materia. Qualora questo non sia immediatamente individuabile, o permangano dubbi sulla corretta assegnazione del documento, l'Ufficio Protocollo invia il documento direttamente alla Segreteria Generale, che provvederà a fornire le indicazioni opportune per il corretto smistamento.

I documenti informatici ed analogici vengono assegnati ai vari Responsabili tramite il sistema di protocollo informatico: qualora un Responsabile del Procedimento riceva un documento non di propria competenza, egli dovrà rifiutarne l'assegnazione o riassegnarlo all'Ufficio competente utilizzando GEDOC oppure contattare l'Ufficio Protocollo.

3.7 RILASCIO DI RICEVUTE

Qualora un documento venga consegnato personalmente, dal mittente o da altra persona incaricata, all'Ufficio Protocollo e venga richiesto il rilascio di una ricevuta attestante l'avvenuta protocollazione, l'Ufficio Protocollo produrrà gratuitamente una fotocopia della ricevuta di protocollazione (timbrata e firmata dall'addetto al Protocollo), riportante il numero progressivo di protocollo e la data, il mittente, l'oggetto, il numero degli allegati e l'impronta informatica del documento.

Qualora per ragioni organizzative o malfunzionamenti del sistema di gestione documentale non sia possibile effettuare subito la protocollazione del documento, l'addetto rilascerà una fotocopia della prima pagina del documento con il timbro di arrivo al Protocollo (V. Allegato n.2). Dal giorno successivo l'interessato potrà richiedere la ricevuta di avvenuta protocollazione.

3.8 CASI PARTICOLARI

a) Lettere anonime

Le lettere anonime non sono registrate al protocollo, ma inoltrate alla Segreteria Generale ed eventualmente, se contengono informazioni o dati di interesse per l'Amministrazione, agli uffici di competenza.

b) Lettere prive di firma

Le lettere prive di firma devono essere protocollate. Sarà poi compito della UOR e, in particolare, del Responsabile del procedimento valutare caso per caso se la lettera priva di firma è da ritenersi valida ai fini della sua efficacia riguardo ad un affare o un determinato procedimento amministrativo.

c) Documenti di competenza di altre amministrazioni

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

d) Originali plurimi (ad esempio comunicazioni identiche indirizzate a più destinatari interni all'ente e riportanti lo stesso numero di protocollo) che pervengono in tempi successivi: viene protocollato solo il primo esemplare pervenuto che viene trasmesso a tutti i destinatari presenti sul documento. Sugli altri originali viene apposto il timbro di protocollo e inserito lo stesso numero già attribuito.

e) Documenti privi di allegati.

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

3.9 TRASMISSIONE DEI DOCUMENTI ANALOGICI IN USCITA

Nei casi in cui si rende necessario procedere alla spedizione della copia di un documento su supporto cartaceo, essa deve essere inviata dall'Ufficio interessato, unitamente all'occorrente per la spedizione (buste indirizzate, ricevute di ritorno già compilate, ecc.) all'Ufficio Posta, che provvede alla spedizione.

SEZIONE IV – IL SISTEMA DI PROTOCOLLO INFORMATICO

4.1 LA REGISTRAZIONE DEI DOCUMENTI NELL'APPLICAZIONE "GEDOC"

Il sistema di Gestione documentale "GEDOC" permette la di svolgere funzionalità ulteriori rispetto alle semplici operazioni di registrazione e di classificazione dei documenti. Il sistema è infatti integrato con funzionalità aggiuntive necessarie alla gestione dei flussi documentali, alla conservazione dei documenti e all'esibizione a norma. I documenti informatici sono memorizzati dal sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo. Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio degli scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.

Gli utenti del servizio di protocollo, in base agli Uffici di appartenenza e alle rispettive competenze, hanno autorizzazioni di accesso differenziate. Ad ogni utente è assegnata:

• una credenziale di accesso, costituita da una componente:

– pubblica che permette l'identificazione dell'utente da parte del sistema (userID);

– privata o riservata di autenticazione (password);

• un profilo, al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione (profili) sono assegnati agli utenti dal Responsabile del Servizio, che si avvale di un utente privilegiato (Amministratore).

4.2 ELEMENTI OBBLIGATORI E FACOLTATIVI DELLA REGISTRAZIONE DI PROTOCOLLO

Il protocollo è composto da elementi obbligatori e da elementi facoltativi. La registrazione degli elementi obbligatori del protocollo è rilevante sul piano giuridico-probatorio mentre la registrazione degli elementi facoltativi del protocollo è rilevante sul piano organizzativo-gestionale.

Gli elementi obbligatori della registrazione di protocollo, cioè quelli rilevanti sul piano giuridico-probatorio, sono:

a) il numero di protocollo generato automaticamente dal sistema e registrato in forma "non modificabile", costituito da sole cifre;

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

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, generata automaticamente dal sistema e registrata in forma non modificabile, qualora il documento sia stato inviato per via telematica;

g) l'indice di classificazione del documento.

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.

Nel protocollo informatico possono venire registrati elementi facoltativi il cui scopo è di rendere quanto più efficace ed efficiente l'azione amministrativa; questi elementi assumono rilevanza solo sul piano organizzativo e gestionale. La Camera di Commercio di Genova valorizza i seguenti dati:

a) data di arrivo (nel formato giorno/mese/anno);

b) luogo di provenienza o di destinazione del documento;

c) tipo di spedizione.

4.3 ANNULLAMENTO O MODIFICA DI UNA REGISTRAZIONE DI PROTOCOLLO

Nell'ipotesi in cui si dovesse ricorrere alla modifica anche di una sola delle informazioni generate o assegnate in maniera automatica dal sistema (numero e data di protocollo), è necessario annullare l'intera registrazione. L'annullamento di una registrazione a protocollo è consentita solo al Responsabile del Servizio Affari Generali - Protocollo, tramite l'utilizzo di una apposita funzione del sistema di protocollo informatico della Camera di Commercio. L'operazione avviene attraverso l'apposizione, da parte del sistema di Gestione Documentale, di un apposito segno grafico sulla registrazione di protocollo. Il sistema di protocollo informatico consente, comunque, agli utenti opportunamente abilitati, la lettura di tutte le informazioni precedentemente registrate.

Nel caso di eventuale modifica anche di una sola delle altre informazioni registrate, per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, il sistema, contestualmente all'aggiornamento del dato con i valori corretti, memorizza nella banca dati il contenuto precedente assieme alle informazioni relative alla data, l'ora ed all'autore della modifica.

4.4 IL 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 contenuto del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno, è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, che ne garantisce l'immodificabilità del contenuto (v. paragrafo n.6.5).

4.5 REGISTRO DI EMERGENZA

Il Responsabile della Gestione Documentale autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora d'inizio dell'interruzione nonché la data e l'ora di ripristino della funzionalità del sistema. Le unità di personale autorizzate alla registrazione dei documenti su registri di emergenza sono le unità appartenenti all'Ufficio Protocollo abilitate alla protocollazione.

Il Responsabile della Gestione Documentale tiene i registri di emergenza, su cui effettua le necessarie annotazioni. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattr'ore, per cause di eccezionale gravità, il Responsabile della Gestione Documentale può autorizzare l'uso del registro di emergenza per periodi successivi della durata massima pari a una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. Per ogni giornata di registrazione manuale è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. La sequenza numerica utilizzata sul registro di emergenza costituisce una sequenza autonoma e riparte dal n. 1 per ogni anno di utilizzo. La sequenza numerica anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico, dal numero successivo all'ultimo registrato prima dell'interruzione.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

SEZIONE V - ORGANIZZAZIONE E GESTIONE DELL'ARCHIVIO CORRENTE (CLASSIFICAZIONE E FASCICOLAZIONE)

5.1 TITOLARIO DI CLASSIFICAZIONE

Per titolario di classificazione si intende sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi. Il titolario di classificazione si suddivide in categorie, le quali si suddividono in classi e sottoclassi. Il titolario di classificazione delle Camere di Commercio è stato elaborato nel dicembre 2000 da un apposito gruppo di lavoro (Sottocommissione per la revisione del titolario d'archivio) costituito all'interno del Comitato Tecnico Scientifico per gli Archivi delle Camere di Commercio, ed è stato adottato con deliberazione della Giunta camerale n.52 del 19.02.2001.

Il titolario svolge essenzialmente due funzioni: da un lato esso consente di collegare tra loro i documenti attinenti ad un determinato affare di competenza dell'Ente, aggregandoli materialmente in un fascicolo (creazione dei fascicoli); dall'altro consente di mantenere il legame tra fascicoli omogenei (archiviazione dei fascicoli).

Ai fini di una corretta classificazione dei documenti vale la seguente regola generale: è il titolo della categoria a contraddistinguere le classi della stessa e quindi a guidare la classificazione dei documenti, dal generale al particolare. Per individuare la categoria corretta e la relativa classe occorre considerare la funzione del documento, il suo oggetto, il procedimento cui appartiene. Pertanto, il processo di classificazione consiste nel determinare per ciascun documento la materia o affare cui esso prende parte e nell'identificare nel titolario la corrispondente categoria, classe e sottoclasse. Sono consentite classificazioni multiple (di norma non più di due) qualora uno stesso documento riguardi più procedimenti amministrativi o funzioni. In tal caso, il documento viene duplicato e inserito nei fascicoli afferenti i diversi procedimenti.

5.2 IL FASCICOLO: INDIVIDUAZIONE, GESTIONE E TENUTA

Tutti i documenti sono riuniti in fascicoli elettronici nel sistema di Gestione documentale GEDOC: è infatti possibile gestire la fascicolazione dei documenti informatici (protocollati o meno) costituendo un vero e proprio archivio informatico integrato con il sistema di conservazione digitale. La scansione a norma dei documenti cartacei, possibile grazie alla dichiarazione di conformità all'originale apposta dall'addetto alla protocollazione e firmata digitalmente, consente di archiviare documenti informatici in modo conforme alla normativa vigente, allo scopo di mantenerne l'integrità, l'autenticità e la leggibilità nel tempo.

Il fascicolo costituisce l'unità di base di un archivio, fondamentale per la gestione e la conservazione della documentazione relativa a ciascun procedimento. Un fascicolo è costituito dal raggruppamento organico di documenti relativo a uno stesso oggetto (procedimento, processo, materia, forma/tipo del documento) e identificato da un codice alfanumerico dato dall'indice di classificazione e dal numero progressivo dell'unità/fascicolo. Ogni documento, una volta assegnato alla struttura organizzativa di competenza, va fascicolato a cura del Responsabile del procedimento. I documenti contenuti nel fascicolo sono ordinati cronologicamente in modo che quello più recente compaia per primo.

Con l'inserimento nel fascicolo il documento viene ad essere classificato acquisendone lo stesso indice di classificazione.

Tutti i documenti ricevuti o prodotti dall'Ente camerale devono essere riuniti in un fascicolo elettronico, indipendentemente dal supporto sul quale sono formati. La formazione di un nuovo fascicolo avviene con l'operazione di apertura che comporta la registrazione delle seguenti informazioni:

a) l'anno di apertura;

b) l'anno di chiusura;

c) l'indice di classificazione del titolario;

d) il numero del fascicolo;

e) l'oggetto, inteso come stringa di testo che descrive compiutamente il contenuto del fascicolo.

L'indice di classificazione è costituito dalla categoria, classe ed eventuale sottoclasse.

5.3 TIPOLOGIE DI FASCICOLI

I fascicoli si dividono in tre tipologie:

- fascicoli relativi ad affari o procedimenti amministrativi;
- fascicoli del personale;
- fascicoli anagrafici.

5.3.1 FASCICOLI RELATIVI A PROCEDIMENTI AMMINISTRATIVI

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo e sottofascicolo di competenza. L'operazione va effettuata dal responsabile del procedimento amministrativo.

I documenti sono archiviati all'interno di ciascun fascicolo o sottofascicolo, secondo l'ordine cronologico di registrazione, in base, cioè, al numero di protocollo ad essi attribuito o, se assente, in base alla propria data.

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. Qualora insorgano esigenze pratiche, il fascicolo può essere distinto in sottofascicoli, i quali a loro volta possono essere distinti in inserti. Il fascicolo viene chiuso al termine del procedimento amministrativo. La data di chiusura si riferisce alla data dell'ultimo documento inserito nel fascicolo.

5.3.2 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, salvo inserimenti di atti

posteriori. I fascicoli del personale costituiscono una serie archivistica, da conservare in ordine alfabetico per cognome e nome. I fascicoli del personale in servizio fanno parte dell'archivio corrente e sono conservati presso l'Ufficio del Personale in armadi chiusi a chiave, quelli attinenti il personale cessato vengono trasferiti all'archivio di deposito.

5.3.3 FASCICOLI ANAGRAFICI (REGISTRO IMPRESE, ALBI, ECC.)

Il Fascicolo Anagrafico, viene aperto al momento della presentazione della domanda di iscrizione al Registro Imprese o ad Albi, Elenchi, Ruoli tenuti dalla Camera di Commercio. Il fascicolo viene chiuso al momento in cui viene accertata la cessazione dell'attività, sia previa domanda che d'ufficio (dietro segnalazione di altri enti, decesso del titolare ecc.)

I fascicoli anagrafici costituiscono una serie archivistica da conservare in ordine di numero REA - Repertorio Economico Amministrativo.

SEZIONE VI - CONSERVAZIONE DEI DOCUMENTI ANALOGICI (ARCHIVIO CORRENTE E DI DEPOSITO)

6.1 ARCHIVIO CORRENTE E ARCHIVIO DI DEPOSITO

L'archivio corrente è costituito dai documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione ovvero conclusi da un breve periodo di tempo e che perciò rivestono ancora un forte interesse ai fini dello svolgimento dell'attività corrente. Esso è collocato di norma presso le singole Unità Organizzative Responsabili.

L'archivio di deposito è formato dai documenti semi-attivi, cioè relativi ad affari e a procedimenti amministrativi conclusi da meno di 40 anni e verso i quali sussistono saltuarie esigenze di consultazione ai fini dell'attività corrente. L'accesso all'archivio di deposito, conservato in appositi locali adeguatamente attrezzati presso la sede di Via Dassori 51 a Genova, è consentito al solo personale autorizzato.

6.2 VERSAMENTO DEI FASCICOLI CARTACEI NELL'ARCHIVIO DI DEPOSITO

Periodicamente i singoli Uffici individuano i fascicoli cartacei relativi ad affari e procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti.

I fascicoli così individuati sono trasferiti all'archivio di deposito, accompagnati da una nota di trasmissione sottoscritta dal responsabile dell'Ufficio, nella quale sono indicati il numero delle unità archivistiche (fascicoli, faldoni, registri) trasferite, la classificazione, l'oggetto e l'anno (o gli anni) di riferimento. Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie hanno nell'archivio corrente.

All'atto del ricevimento il personale addetto al Servizio, dopo aver verificato la corrispondenza tra il materiale consegnato e la nota di trasmissione, provvede all'aggiornamento dell'"Elenco di consistenza dell'archivio di deposito" e alla collocazione dei documenti secondo l'organizzazione dell'archivio.

I fascicoli del personale dipendente vengono versati dall'archivio corrente all'archivio di deposito non prima di 5 anni dalla data di cessazione dal servizio del dipendente.

Le serie e i repertori delle delibere sono conservati presso l'Ufficio Protocollo e Affari Generali a partire dall'anno 1935.

Le serie delle determinazioni dirigenziali dal 1999 ad oggi sono conservate presso l'Ufficio Protocollo e Affari Generali.

6.3 CONSULTAZIONE E MOVIMENTAZIONE DEI FASCICOLI

L'affidamento temporaneo di un fascicolo, già trasferito all'archivio di deposito, ad una Unità Organizzativa Responsabile o a personale autorizzato deve avvenire per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo. L'affidamento temporaneo avviene mediante richiesta trasmessa via email contenente i motivi e la firma del richiedente. Un esemplare della richiesta è conservato dall'Ufficio Archivio e protocollo, l'altro è inserito nella posizione fisica occupata dal fascicolo in archivio.

Il personale addetto all'Archivio tiene traccia di tale movimentazione nel Registro di carico e scarico dei fascicoli, nel quale riportare il nominativo del richiedente, la motivazione, la data della richiesta, la data della restituzione ed eventuali note sullo stato della documentazione così come si consegna e così come viene riconsegnata.

Non è consentita l'estrazione di documenti in originale dal fascicolo, che vanno tenuti in ordine di sedimentazione rispettando il vincolo archivistico, cioè l'appartenenza di ogni documento alla rispettiva unità archivistica (fascicolo, sottofascicolo).

6.4 - SELEZIONE DEI DOCUMENTI - SCARTO ARCHIVISTICO

Periodicamente – almeno ogni due anni – il Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi provvede alla selezione dei documenti finalizzata alla loro conservazione o al loro scarto, secondo le prescrizioni del Massimario di selezione in uso e nel rispetto della normativa vigente in materia.

6.4.1 MASSIMARIO DI SELEZIONE

L'individuazione dei documenti per la conservazione o lo scarto avviene sulla base del "Massimario di conservazione e scarto per gli archivi camerali", predisposto dal Ministero dell'Industria Commercio e Artigianato e recepito dalla Camera di Commercio con determinazione del Segretario Generale n.382/Z del 15 dicembre 2014, che definisce, per ciascuna voce del titolario d'archivio, le principali tipologie documentarie e i relativi tempi di conservazione. Ad ogni titolario di classificazione corrisponde un massimario di selezione.

6.4.2 PROCEDURE DI SELEZIONE

Il Segretario Generale con apposito provvedimento istituisce la Commissione preposta ad effettuare lo scarto degli atti di archivio.

La selezione dei documenti viene effettuata utilizzando il Massimario. La Commissione predispone l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico. La proposta di scarto viene sottoposta ai responsabili delle UO interessate per eventuali osservazioni. Qualora la UO lo ritenga necessario, in seguito a richiesta scritta e motivata sottoscritta dal Responsabile, è consentita la conservazione dei documenti per un periodo di tempo maggiore rispetto a quello previsto dal massimario. I documenti così cancellati dalla proposta di scarto vengono riportati nell'elenco dell'anno successivo.

La proposta di scarto è approvata con Determinazione del Segretario Generale, successivamente trasmessa alla Soprintendenza Archivistica per la Regione Liguria per il nulla osta.

Successivamente al ricevimento del nulla osta, il materiale da scartare è consegnato a ditte specializzate per la distruzione. Delle operazioni di distruzione è redatto apposito verbale. Una copia dello stesso è trasmessa per conoscenza alla Soprintendenza Archivistica che ha autorizzato lo scarto.

6.5 CONSERVAZIONE DEI DOCUMENTI

La documentazione corrente è conservata a cura del Responsabile del procedimento fino al trasferimento in archivio di deposito. I documenti che costituiscono l'Archivio di deposito sono conservati e custoditi in appositi locali opportunamente attrezzati con scaffalature e armadi, ai quali può avere accesso soltanto il personale dell'Ufficio Archivio e Protocollo. L'Archivio di deposito è suddiviso in sezioni corrispondenti ai diversi titolari di classificazione ed è gestito tramite un Elenco di consistenza.

6.6 ARCHIVIO STORICO

I documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni sono trasferiti alla sezione storica per la conservazione permanente contestualmente agli strumenti che ne garantiscono l'accesso (Inventari). Presso l'Archivio di Stato competente per territorio, secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali, sono conservati i documenti della Camera di commercio di Genova dall'anno 1805, anno della sua fondazione.

SEZIONE VII – SICUREZZA

7.1 PIANO PER LA SICUREZZA INFORMATICA

Le misure di sicurezza adottate dalla Camera di Commercio di Genova per la formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali, sono contenute nel Piano per la sicurezza informatica, adottato nel 2015 e aggiornato con determinazione n.486/Z del 26.11.2018 (v. Allegato n.3).

7.2 SICUREZZA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Per quanto riguarda nello specifico il sistema operativo per la gestione documentale GEDOC, fornito da Infocamere S.c.p.A., esso è configurato in modo tale da consentire:

• l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti presenti al di fuori del sistema di gestione documentale;

• la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

• garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

• garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

• fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

• consente il reperimento delle informazioni riguardanti i documenti registrati;

• garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Il Responsabile della Gestione Documentale è la persona che ha la possibilità di effettuare operazioni sul sistema, come, a titolo esemplificativo:

• predisporre le autorizzazioni di accesso al sistema;

• eseguire la stampa del registro di protocollo giornaliero;

• monitorare tutte le operazione compiute.

• procedere all'annullamento dei protocolli.

Il Responsabile della Gestione Documentale ha accesso a tutti i dati del protocollo.

7.2.1 DEFINIZIONE DEI DIRITTI DI ACCESSO E PROFILI UTENTE

Operatore di Protocollo

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

A tutti i documenti protocollati in arrivo l'operatore di protocollo attribuisce la classificazione (categoria e classe).

Gli operatori di protocollo assegnati all'Ufficio Protocollo hanno la visibilità totale nel sistema di gestione documentale GEDOC, vale a dire che sono in grado di prendere visione di tutti i protocolli registrati, indipendentemente dalla loro posizione nell'organigramma. Gli operatori di protocollo decentrati in altri uffici invece possono consultare solo i protocolli assegnati all'Ufficio di appartenenza.

Utente abilitato alla consultazione

L'utente consultatore è abilitato ad accedere al protocollo informatico limitatamente ai documenti assegnati ad esso agli Uffici o Servizi di propria competenza. Il sistema consente di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione: i documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Visibilità dei protocolli

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

• I protocolli devono essere visibili dall'utente che li ha inseriti e da quelli con pari abilitazioni (cioè appartenenti alla stessa UO o a UO collocata gerarchicamente ad un livello superiore nell'organigramma)

• La visibilità dei protocolli deve essere piramidale: Il Segretario Generale ha visibilità su tutti i protocolli; ogni Dirigente può vedere i protocolli di tutta la propria Area (quindi i propri e quelli dei propri Servizi, Uffici, Addetti); ogni Responsabile di Servizio può vedere i protocolli di tutto il Servizio (quindi i propri e quelli dei propri Uffici, Addetti); il Responsabile di un Ufficio può vedere i protocolli propri e quelli dei propri Addetti.

• Se un Addetto svolge funzioni per Uffici diversi, quando entra nel sistema di gestione documentale deve effettuare una scelta per decidere per quale Ufficio consulta il sistema.

- Il sistema di Gestione documentale GEDOC consente anche l'attribuzione della visibilità su un documento o fascicolo specifico ad un utente singolo (e non alla UO a cui appartiene)

7.3 CONSERVAZIONE A NORMA DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avviene con le modalità e le regole tecniche specificate nel DPCM 3 dicembre 2013. Il processo di conservazione è stato delegato ad un soggetto esterno, Infocamere (Conservatore Accreditato presso l'Agenzia per l'Italia Digitale), che fornisce il sistema di gestione documentale GEDOC, il quale consente di effettuare, oltre alla registrazione:

- la conservazione del documento: il documento, ricevuto nel Data Center di InfoCamere in formato digitale, viene conservato a norma di legge per tutta la durata prevista per la conservazione;

- la rettifica di un documento conservato: un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica non comporta la cancellazione del documento originario dall'archivio a norma, nel pieno rispetto del principio di tracciabilità del documento;
- la cancellazione di un documento conservato: un documento inviato in conservazione può essere cancellato, allegando eventualmente la motivazione della cancellazione. Il sistema terrà comunque traccia del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità del documento;
- l'esibizione (a norma) di un documento conservato: il documento richiesto viene richiamato direttamente dal servizio di gestione documentale ed esibito con garanzia della sua opponibilità a terzi;
- la conservazione forzata di un lotto di documenti nel caso in cui si debba derogare alle modalità standard di chiusura del processo di conservazione;
- la gestione dei visualizzatori dei documenti conservati e l'ottenimento d'informazioni di stato su documenti e lotti conservati.

SEZIONE VIII - DISPOSIZIONI TRANSITORIE E FINALI

8.1 MODALITÀ DI ADOZIONE INIZIALE E DEGLI AGGIORNAMENTI AL MANUALE

Il Manuale di gestione è approvato con deliberazione della Giunta camerale.

8.2 MODALITÀ DI COMUNICAZIONE DEL MANUALE

La Camera adempie all'obbligo di comunicazione del Manuale stesso mediante la pubblicazione sul proprio sito internet.

8.3 MODALITÀ DI AGGIORNAMENTO DEL MANUALE

Periodicamente possono essere apportati aggiornamenti al Manuale di Gestione. Gli aggiornamenti possono riguardare anche solo una sezione o allegato del Manuale.

Gli aggiornamenti aventi ad oggetto gli allegati al Manuale potranno essere adottati con provvedimento del Segretario Generale.

ALLEGATI

- N.1 - ORGANIGRAMMA GEDOC
- N. 2 - TIMBRI DI PROTOCOLLO E DI ARRIVO ALL'UFFICIO PROTOCOLLO
- N.3 - PIANO PER LA SICUREZZA INFORMATICA
- N.4 - METADATI ASSOCIATI AI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Organigramma

- AOO000
  - Segretario Generale
    - UFFICIO SEGRETERIA GENERALE
    - SEGRETERIA PRESIDENZA
    - SETTORE TURISMO E RELAZIONI ESTERNE
    - SERVIZIO AFFARI GENERALI E PROTOCOLLO
      - Affari generali - Protocollo
      - Biblioteca
    - DIR.SETTORI RAGIONERIA E BILANCIO / PROVVEDITORATO
    - PROVVEDITORATO
      - Ufficio Provveditorato
      - UFFICIO POSTA
    - RAGIONERIA E BILANCIO
      - Ufficio Contabilita e Bilancio
      - Tributi
      - C.E.D.
    - DIR.II: ATTIVITA PROMOZIONALI
      - Istituto di Economia Internazionale
      - Settore servizi alle attivita produttive e commerciali
      - Settore Servizi Innovativi
        - REC
        - Borsa merci
      - PROMOZIONE AGRICOLTURA E ARTIGIANATO
      - Settore Internazionalizzazione
      - Settore Logistica
        - PROMOZIONE SETTORE MARITTIMO
        - PROMOZIONE TRASPORTI
      - SETTORE CREDITO USI E PROTESTI
        - CREDITO
        - Protesti
        - USI
    - DIR. III: SERVIZI ANAGRAFICI
    - SETTORE REGISTRO IMPRESE - ARTIGIANATO
      - Albo Imprese Artigiane
      - Ufficio Registro Imprese
      - Ruolo Agenti e Rappresentanti di Commercio

- Ufficio orientamento al lavoro
- SETTORE AMBIENTE E ABILITAZIONI SPECIALI
- UFFICIO AMBIENTE
- m.u.d.
  - Registro Pile
  - Sottoprodotti
  - Registro A E E
- UFFICIO ABILITAZIONI SPECIALI
  - Registro F Gas
- SEZIONE CHIAVARI ED EVENTI ALLUVIONALI
- SEZIONE DI CHIAVARI
- UFFICIO ALLUVIONI 2010-2014
- DIR.V: REGOLAZIONE DEL MERCATO
- SETTORE SERVIZI REGOLAZIONE DEL MERCATO
- Camere Arbitrali - Usi - Conciliazione
- UFFICIO SANZIONI AMMINISTRATIVE
- RUOLI - ELENCHI
  - MEDIATORI MARITTIMI
  - PERITI ED ESPERTISPEDIZIONIERIRACC.MARITT.PESATORISTIMATORI
  - RUOLO AGENTI DI AFFARI IN MEDIAZIONE
- SETTORE INNOVAZIONE
- RAO
- Ufficio metrico
- DIR. PERSONALE
- UFFICIO CONTROLLO DI GESTIONE
- SERVIZIO INTEGRATO DEL PERSONALE
- Settore Personale e Organizzazione
- Trattamento Economico del Personale
- SETTORE STATISTICA E PREZZI
- UFFICIO STUDI
- UFFICIO STATISTICA

Allegato n.2

timbro di arrivo
all'ufficio Protocollo

timbro di protocollo

PIANO PER LA SICUREZZA INFORMATICA

Il Piano per la sicurezza informatica (art.4, comma 1, lett. c) del D.P.C.M. 3 dicembre 2013) è redatto in ottemperanza delle misure minime previste dall'allegato B del Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003 n. 196).

Occorre premettere che la gestione informatica dei dati di cui la Camera è titolare è realizzata, in modo prevalente, tramite i prodotti e i servizi erogati da Infocamere S.c.p.A. (Società consortile di informatica delle Camere di commercio italiane), o da società ad essa collegate (nominate dalla Camera Responsabili del trattamento ai sensi dell'art. 4, comma 1, lett. g) del Codice Privacy) e sulla rete di trasmissione dati (IC rete) gestita da Infocamere in ambito nazionale per l'archiviazione e la trasmissione dei dati facenti parte del patrimonio informativo delle camere di commercio. La Camera opera nella rete Infocamere che la società gestisce sotto tutti i profili, compreso quello della sicurezza. Si rinvia pertanto ai documenti prodotti dalla Società per la descrizione di tutti i relativi aspetti.

1- Definizione dell'ambito con riferimento al trattamento elettronico dei dati

Gli archivi gestiti elettronicamente con strumenti informatici comprendono sia banche dati gestite internamente che banche dati gestite dalla Società consortile Infocamere o altre società del gruppo.
Per l'analisi dei rischi e le prescrizioni per la sicurezza delle banche dati gestite da Infocamere e dalle altre società del gruppo, e da Infocert spa si rinvia ai documenti redatti dalle società, nominate dalla Camera Responsabili del trattamento.

Rientrano nell'ambito sopradescritto i trattamenti gestiti con strumenti informatici da soggetti esterni ma facenti capo alla rete camerale e, per quanto riguarda la posta elettronica, ai server della Camera di Genova e cioè l'Unione regionale delle Camere di Commercio della Liguria in liquidazione, con sede in Via San Lorenzo 15 (entro il 2018 è in previsione il trasferimento presso la sede camerale di P.zza De Ferrari 2) e il CLP – Centro ligure produttività, con sede presso la Camera di Genova in Via Boccardo, associazione senza scopo di lucro, costituita presso la Camera e dalla stessa sostenuta. Rientrano nell'ambito sopradescritto anche i trattamenti gestiti dalla Azienda speciale 'inHouse' – istituita dalla Camera di commercio di Genova con delibera n. 19 del 04.02.2008 e affidataria, presso la sede dell'Ente, di attività implicanti accesso a banche dati e archivi camerali. Tali organismi sono pertanto tenuti a garantire il rispetto delle misure di sicurezza, adottate dalla Camera di Genova e descritte nel presente documento o comunque necessarie (ad es. tutela degli accessi) per contrastare i rischi cui può essere sottoposto il sistema informativo e a consentire da parte della Camera adeguata attività di vigilanza e controllo.

2 - Misure di sicurezza

Nella presente sezione sono illustrate le misure individuate ai fini di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
In quanto tale si intende descrivere, con le misure di sicurezza in essere, un quadro di riferimento organico che possa risultare utile per il perfezionamento e l'aggiornamento nel tempo di

procedure, modalità, regole e prescrizioni in materia e per operazioni di verifica e controllo da attuarsi periodicamente.

2.1 Apparecchiature informatiche critiche

Sono considerate apparecchiature informatiche critiche quelle apparecchiature che vengono utilizzate per il trattamento di dati personali.

- Computer (sia server che workstation);
- Unità input/output accessorie a dischi ottici o magnetici e unità nastri.
- Sistemi per la gestione delle LAN (router, hub, switch, ecc.).

Tali apparecchiature sono collocate in aree ad accesso riservato.
Le apparecchiature delle LAN non facenti parte del backbone e che non possono essere situate nelle aree ad accesso controllato, sono riposte all'interno di armadi metallici chiusi.

2.2 Supporti di memorizzazione critici

Sono considerati supporti di memorizzazione critici i nastri magnetici, le cassette (cartridge), i dischi magnetici o ottici rimovibili, i CD-ROM e DVD, HD, chiavi USB ecc. che contengono informazioni personali.
I supporti di memorizzazione critici devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato e comunque in un armadio/cassetto chiuso a chiave.

2.3 Informazioni residue

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento (es. nastri, dischi magnetici, dischi ottici, HD, chiavi USB ecc.).
Le informazioni residue devono essere rese inaccessibili e illeggibili quando non sia più necessario conservarle per gli scopi per cui i dati sono stati raccolti e trattati. In caso di dismissione di apparecchiature o supporti - sia che se ne preveda lo smaltimento sia il riciclo – vanno osservate le prescrizioni dettate dal Garante con provvedimento del 13 ottobre 2008 (Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali) e le misure tecniche suggerite negli allegati al provvedimento citato o successivamente indicate per la cancellazione sicura delle informazioni.

3 - Sicurezza logica. Prescrizioni generali

Questa sezione disciplina i diversi aspetti del controllo dell'accesso logico alle informazioni personali, Quale principio generale, sono regolamentati gli accessi ai server, alle workstation, alle LAN, alla rete e alle banche dati del Sistema Informatico Camerale attraverso funzioni di identificazione e autenticazione degli utenti.
Tale funzioni assicurano che ad ogni potenziale utente dei sistemi o delle banche dati siano associate delle credenziali di autenticazione consistenti in un codice per l'identificazione (user-id) ed una parola chiave riservata (password), conosciuta solo dall'utente medesimo, oppure di un dispositivo di autenticazione in possesso e uso esclusivo dell'utente. Tali credenziali o dispositivi di autenticazione consentono, ad ogni accesso dell'utente alla rete, al sistema o alla banca dati, di verificarne l'identità e di garantirne l'accesso ai dati di cui è incaricato tramite il sistema di autorizzazione agli accessi.

3.1 - User-id

L'accesso ai sistemi, alle banche dati contenenti informazioni personali, o alla rete deve essere basato sulle effettive necessità del trattamento. Per ragioni meramente tecniche, ad ogni utente possono essere assegnate una o più credenziali per l'autenticazione.
In ogni caso, le user-id assegnate devono sempre essere riconducibili ad un singolo individuo e non possono essere assegnate ad altri utenti neppure in tempi diversi.
Le credenziali ed i dispositivi di autorizzazione sono custoditi con particolare perizia e cautela sotto la responsabilità personale degli utenti consegnatari.
Le credenziali ed i dispositivi di autorizzazione non utilizzati, ad eccezione di quelli creati per scopi tecnici, devono essere disattivati.

3.2 Assegnazione e revoca delle user-id ed abilitazioni

La procedura tecnica per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati ed alla rete del Sistema Informatico Camerale viene normalmente gestita da Infocamere. Può essere gestita propriamente dall'Ente nel caso in cui si tratti di accessi a sistemi e banche dati gestiti direttamente dall'Ente. Parimenti, per i sistemi e banche dati gestiti da terzi (diversi da Infocamere), questi normalmente provvedono all'assegnazione delle relative credenziali di autorizzazione all'accesso. L'abilitazione con la connessa individuazione di uno specifico profilo di autorizzazione all'accesso, avviene in ogni caso su richiesta diretta del responsabile della struttura cui appartiene l'incaricato che ne deve essere titolare.
Quando un utente non ha più la necessità di accedere ad una banca dati, lascia l'Ente o comunque non utilizza da almeno sei mesi le credenziali, il diretto superiore dell'utente interessato provvede a richiedere al soggetto che ha rilasciato le credenziali di autorizzazione la disabilitazione dell'utenza.
Le user-id attribuite da Infocamere, per l'accesso alla rete o per procedure gestite dalla stessa o da società del gruppo, e da Infocert, qualora siano inutilizzate per più di 6 mesi, vengono automaticamente disattivate.
Non è consentito il riutilizzo di una user-id personale già assegnata ad altro utente.

3.4 Password

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati ed un corretto utilizzo delle stesse rappresenta un pilastro fondamentale nella gestione complessiva della sicurezza, anche nell'ottica di garanzia e tutela degli utenti.
Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation tramite le quali si può accedere alla rete ed alle banche dati contenenti dati personali.
Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

3.5 Regole delle password

- La lunghezza minima della password è di 8 caratteri;
- Deve contenere almeno un carattere alfabetico ed uno numerico;
- Non deve essere simile alle due password precedenti;
- Non deve contenere l'user-id come parte della password;
- Non deve contenere riferimenti agevolmente riconducibili all'utente;
- Deve essere cambiata al primo utilizzo ed almeno ogni 6 mesi (3 mesi se afferente dati sensibili o giudiziari);
- Non deve essere comunicata ad altri utenti.

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

3.6 Ripristino della password

Il ripristino della password, in caso di blocco della stessa, deve essere effettuato dagli amministratori di sistema solo a fronte di una diretta richiesta da parte dell'intestatario, rispettando le istruzioni e nei casi all'uopo previsti. La password dovrà essere cambiata subito dopo a cura del richiedente.

3.7 Utilizzo delle password

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

- richiesta dal sistema operativo nella fase di avvio del computer;
- richiesta quando si intende accedere alla rete (sia Intranet che Internet);
- richiesta per l'utilizzo di specifiche applicazioni;
- richiesta dal salvaschermo per i momenti in cui si lascia incustodita la postazione di lavoro.

Si devono utilizzare tutti questi livelli di password. Tutte le operazioni inerenti l'utilizzo delle password (digitazione, cambiamento, ecc.) devono essere compiute con estrema cautela e discrezione avendo cura di controllare che tali operazioni non siano visibili a terzi.

3.8 Accesso agli elaboratori in caso di prolungata assenza o impedimento dell'incaricato.

Ferma l'effettuazione della custodia delle copie delle credenziali, con le caratteristiche, anche di segretezza, prevista dall'Allegato B al D.Lgs. n. 196/2003 "Codice in materia di sicurezza dei dati personali ", ai fini dell'accesso da parte del titolare in caso di prolungata assenza o impedimento dell'incaricato si è ritenuto confacente alle esigenze di sicurezza prevedere una procedura consistente in:
-disabilitazione della componente riservata della credenziale per l'autenticazione dell'incaricato assente
-abilitazione di una nuova credenziale che consenta l'accesso al titolare
-configurazione di una nuova credenziale per l'accesso da parte dell'incaricato autorizzato.

Tale procedura potrà essere attuata, per il tramite dell'amministratore di sistema, dando notizia, come prescritto, all'incaricato, dell'evenienza occorsa, e solo in casi di indifferibile necessità di accesso ai dati, su richiesta scritta del titolare o del responsabile. La custodia delle password degli amministratori di sistema è realizzata su supporto cartaceo e formalmente affidata al Provveditore.

3.9 Accesso degli amministratori

In adeguamento alle indicazioni del Garante contenute nel provvedimento del 27/11/2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" si è proceduto, in data 15.12.2009, alla individuazione e nomina degli amministratori di sistema; con successivo provvedimento del 31.07.2015 si è provveduto ad aggiornarne i profili di autorizzazione; sono state adottate user-id nominali per l'autenticazione degli amministratori di sistema ed è stata implementata una procedura di registrazione degli

accessi alla rete da parte degli stessi (access log) conforme alle prescrizioni contenute nel provvedimento citato.

4 - Prescrizioni particolari per la sicurezza logica dei sottosistemi del Sistema Informativo camerale

4.1 Rete

In un sistema integrato, quale quello in cui opera l'Ente, la sicurezza deve essere trattata in modo uniforme, in quanto l'insicurezza di una singola parte si può ripercuotere generando insicurezza in tutto il sistema. Questo vale in particolare per gli aspetti di sicurezza della rete. ICRete, rete geografica del Sistema Informatico Camerale, è gestita da InfoCamere ed InfoCamere stessa ha primariamente il compito di assicurarne la sicurezza.
La Camera di Commercio I.A.A. di Genova collabora con Infocamere per la gestione in sicurezza della parte di rete di propria pertinenza, assicurando che le direttive generali di Infocamere siano rispettate e che siano adottate tutte le ulteriori specifiche fissate dall'Ente.
Per garantire la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa. Per questo qui di seguito sono formulate alcune prescrizioni particolari per le connessioni di ICRete.
Sono considerate connessioni con l'esterno i collegamenti di ICRete con altre reti, in particolare:

- interconnessioni tra i servizi informatici e telematici di InfoCamere e quelli di altre aziende, incluso Internet;
- accesso remoto da parte di dipendenti della Camera o di InfoCamere, secondo le procedure e le stringenti misure di sicurezza stabilite da Infocamere e solo per i soggetti espressamente abilitati.

4.2 Accesso remoto e uso dei modem

Le connessioni via modem tra i sistemi e la rete del Sistema Informatico Camerale con reti e sistemi esterni possono rappresentare un serio rischio per la sicurezza del Sistema stesso. Come conseguenza diretta di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti; nei fatti ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno (e viceversa) deve rispettare i criteri di sicurezza qui esposti. In particolare, nel caso in cui il collegamento sia di tipo TCP/IP tramite modem, non è permesso il suo uso simultaneamente al collegamento interno. Si fa preciso divieto di installare modem.

Si segnala che è in fase di avvio la sperimentazione della modalità di erogazione della prestazione lavorativa denominata "lavoro agile" (prevista dalla l. n.81/2017): un numero di dipendenti non superiore al 10% del totale potrà svolgere la propria attività lavorativa da remoto utilizzando una piattaforma di condivisione approntata da Infocamere ScpA tramite un servizio VPN (Virtual Private Network) che dovrebbe impedire ogni tentativo di accesso fraudolento alla rete camerale.

4.3 Ridondanza nelle apparecchiature di rete e collegamento

Al fine di garantire la massima continuità di servizio possibile tutte le apparecchiature di rete che consentono l'interconnessione con ICRete sono ridondate. E' altresì prevista la possibilità di attivare un collegamento ausiliario di backup nel caso in cui il collegamento principale sia per qualsiasi motivo indisponibile.

4.4 Sistemi e stazioni interconnesse

A livello di singole stazioni interconnesse la gestione della sicurezza è affrontata seguendo due principali filoni

1. Server di applicazioni e dati
2. Workstation

4.5 Server

I server di applicazioni e dati rappresentano nodi fondamentali e altamente strategici del Sistema Informativo Camerale.
Ad essi pertanto è dedicata una particolare attenzione in tema di sicurezza.
Sono collocati esclusivamente in locali ad accesso riservato.
L'accesso agli stessi per effettuare installazioni e configurazioni è possibile solo da parte di personale autorizzato. Fermo quanto previsto dal Provvedimento del 27.11.2008 del Garante, riguardante gli amministratori di sistema, le operazioni di installazione e configurazione dei sistemi sono tracciate in appositi file di log.
In essi è installato un antivirus sempre attivo.
I sistemi operativi sono costantemente aggiornati in modo coerente alle applicazioni che mettono a disposizione, in modo da garantire il più alto livello di sicurezza possibile.
Per ragioni di sicurezza sono tracciati gli accessi (login/logout) alla rete camerale.
Le unità dischi fisse sono ridondate in modo da consentire in maniera istantanea la contestuale scrittura delle informazioni su due diversi supporti fisici (RAID 1, Mirror, o RAID 5, stripe set con parità) e consentire in caso di rottura di uno di essi il ripristino trasparente per l'utente delle informazioni memorizzate.
I server sono collegati a unità atte ad immagazzinare i dati denominate librerie. La camera di commercio dispone di due librerie ridondate in alta affidabilità.
Su di essi è effettuato un backup di sistema e dati attraverso apposite unità a nastro, di norma settimanale, salvo che per determinate tipologie di dati non sia stato previsto un timing minore (es giornaliero o infragiornaliero).
Sono collegati ad un gruppo di continuità che in caso di mancanza di alimentazione elettrica di rete procede all'arresto di tutte le funzioni degli stessi e allo spegnimento

4.6 Workstation

Le workstation, ossia le singole stazioni di lavoro degli utenti, devono avere le seguenti caratteristiche:

- Gli utenti normalmente sono abilitati con un profilo USER salvo che per particolari esigenze o vincoli imposti dalle applicazioni installate non sia necessario attivare profili più potenti, quali Poweruser o Admnistrator.
- In ogni caso, è fatto divieto al personale di installare o disinstallare applicazioni, nonché modificare le configurazioni delle stesse e di accesso al sistema senza darne preventiva comunicazione scritta all'Ufficio CED. L'Ufficio CED valutate tutte le implicazioni in tema di sicurezza e compatibilità delle stesse con l'ambiente di lavoro, qualora non ritenga di dover provvedere in modo diretto, autorizza sotto la propria responsabilità le operazioni di installazione, disinstallazione e riconfigurazione per iscritto.

- Qualora l'Ufficio CED verifichi la presenza sulle stazioni di software non autorizzato è tenuto a darne tempestiva comunicazione scritta alla Dirigenza competente, al fine dell'adozione dei più opportuni provvedimenti. Le informative e comunicazioni per iscritto possono essere effettuate anche tramite messaggi di posta elettronica.
- Le stazioni sono protette da un sistema di antivirus di rete che deve essere sempre attivo e aggiornato. Nel caso in cui l'utente verifichi la temporanea indisponibilità del servizio di antivirus deve darne tempestiva comunicazione all'Ufficio CED che individuerà ed attuerà tutte le azioni necessarie per il ripristino nel tempo più celere possibile delle normali condizioni di sicurezza.
- I sistemi operativi sono aggiornati con tutte le patch di sicurezza testate e compatibili con le applicazioni installate. Tale attività deve essere svolta dall'Ufficio CED in stretta concertazione con i sistemisti ed i responsabili della politica della sicurezza Infocamere.

4.7 Applicazioni

L'utilizzo di applicazioni che consentano di gestire informazioni e dati personali deve avvenire in maniera consapevole e sicura da parte del personale incaricato. Tali requisiti sono soddisfatti attraverso l'effettuazione di peculiari azioni formative sul personale e la strutturazione opportuna delle caratteristiche di funzionamento del software utilizzato.
In particolare, al fine di prevenire al massimo errori accidentali di cancellazione o modifica dei dati le applicazioni che gestiscono informazioni e dati personali devono sempre segnalare adeguatamente la criticità di particolari operazioni effettuate (schema richiesta e successiva conferma).
Tutte le applicazioni che comportano la gestione di informazioni e dati personali e i dati stessi devono essere installate ed archiviati su server posti in aree ad accesso riservato.
Per ognuna di esse e per i relativi archivi devono essere individuati i profili utenti che a vario titolo e con diversi diritti possono interagire con la stessa.
Qualora l'applicazione evidenzi malfunzionamenti od incongruenze nella gestione dei dati, gli incaricati del trattamento devono dare tempestiva comunicazione all'Ufficio CED, che provvederà a verificare gli stessi ed a porre in essere tutte le azioni correttive necessarie.

4.8 Posta elettronica

L'utilizzo di applicazioni di posta elettronica rappresenta un forte fattore di rischio per i sistemi sui quali sono installate in quanto espone gli stessi a minacce dirette derivanti dalle comunicazioni con l'esterno.
Per questo è necessario disciplinare l'utilizzo della stessa in modo da ridurre al massimo i rischi connessi.
Pertanto, quale principio generale, è fatto divieto al personale dell'Ente di utilizzare la rete e le applicazioni installate sulle postazioni di lavoro per finalità diverse da quelle inerenti l'attività dell'ufficio.
La posta elettronica assegnata al personale viene filtrata da un servizio di antivirus centralizzato installato sui server che gestiscono la stessa. Inoltre, su tutte le stazioni gli utenti devono verificare che sia installato ed attivo il servizio di antivirus locale.
Ciò detto, si raccomanda di cancellare immediatamente (anche dal "Cestino") tutti i messaggi provenienti da mittenti non precisamente identificabili e con oggetto non pertinente l'attività dell'ufficio senza visualizzarli direttamente o in anteprima.

Nel caso in cui l'utente rilevi dubbi circa la pertinenza o meno di un messaggio alla propria attività deve informare l'Ufficio CED che provvederà a verificare il contenuto dello stesso in un ambiente sicuro ed isolato da ICRete.
È importante ricordare che la contraffazione dell'indirizzo del mittente nei messaggi di posta elettronica è un'operazione molto semplice. Quindi in generale è opportuno non aprire né tanto meno installare file o programmi ricevuti via posta elettronica da fonti non conosciute o dalle quali non si attendono comunicazioni. Per l'apertura di questi allegati è necessario utilizzare la stessa procedura sopra descritta per la verifica della pertinenza all'attività dell'ufficio dei messaggi ricevuti.

4.9 Dati

Quale principio generale le informazioni contenenti dati personali devono essere archiviate in server posti in locali ad accesso riservato. I dati sono protetti indirettamente anche attraverso la creazione di appositi profili di gestione degli stessi nelle applicazioni e la protezione dell'accesso logico e fisico al repository finale (cartella) in cui sono collocati.
Qualora sia necessario archiviare i dati su singole workstation assegnate agli utenti, devono essere definite particolari misure di sicurezza logica analoghe a quelle adottate sui server, procedure di backup a cura dell'incaricato del trattamento e, sotto la responsabilità dello stesso, le apparecchiature devono essere collocate in uffici od aree chiuse se non presidiate.

4.10 Web filthering

Nel rispetto dello Statuto dei lavoratori e rispettando le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, al fine di ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), la Camera di Commercio ha adottato un sistema di cd. "webfilthering" che si sostanzia in tali aspetti:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il *download* di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

5 - Criteri e modalità di ripristino della disponibilità dei dati

5.1 Introduzione

La presente sezione si pone come obiettivo quello di descrivere i criteri e le procedure adottate per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.

Il principio generale adottato dall'Ente in tal ambito è che tutti i database contenenti dati personali, devono essere archiviati esclusivamente sui server dati appositamente creati e predisposti allo scopo. Su di essi devono confluire anche tutti gli elenchi, query e report estratti da banche dati gestite da Infocamere o terzi che contengano dati personali ed anche le informazioni interne riservate e confidenziali prodotte dagli uffici.

Sulle singole workstation possono essere memorizzate informazioni e dati di lavoro temporanei di non particolare rilevanza in modo tale che la loro eventuale perdita, distruzione o alterazione non comporti alcun pregiudizio al rispetto delle politiche di sicurezza adottate.
Sui server è automaticamente implementata una politica di sicurezza con dischi ridondati (RAID 1, Mirror, o RAID 5, stripe set con parità) e di backup pianificato.
Per le finalità del presente documento si definisce "insieme omogeneo di dati" ogni singola cartella generale collocata sui server che può contenere basi dati, sottocartelle contenenti dati o semplici file aventi una qualche relazione definita fra loro e quindi collocati nel medesimo ambito.

5.2 Backup

Le procedure di salvataggio delle banche dati avvengono con cadenza giornaliera; si è optato per un backup totale dei dati con quattro set di cassette. Ogni set ha la capienza di una settimana. I set vengono gestiti in rotazione in modo che sia a disposizione un salvataggio sino al mese precedente.

5.3 Ripristino

I backup effettuati tramite supporto a nastri sono soggetti, periodicamente ed a campione, ad una procedura di ripristino che verifichi la bontà del backup effettuato e l'effettiva accessibilità ai dati archiviati.

Documenti soggetti a registrazione particolare e relativi metadati (art.5, c.2, lett. e) DPCM 3 dicembre 2013)

tipologia del documento	metadati del documento	UO competente
delibere delle Giunta camerale	tipo Atto, Ufficio Redattore, Oggetto, Fase, Data di presentazione, Data di numerazione, Numero Provvisorio, Numero Definitivo, Provvedimenti contabili (Sì/No), Riservato (Sì/No)	Ufficio Affari Generali e Protocollo
delibere del Consiglio camerale	tipo Atto, Ufficio Redattore, Oggetto, Fase, Data di presentazione, Data di numerazione, Numero Provvisorio, Numero Definitivo, Provvedimenti contabili (Sì/No), Riservato (Sì/No)	Ufficio Affari Generali e Protocollo
determinazioni dirigenziali	tipo Atto, Sottitipo, Ufficio Redattore, Categoria, Oggetto, Fase, Data di presentazione, Data di numerazione, Numero Provvisorio, Numero Definitivo, Provvedimenti contabili (Sì/No), Riservato (Sì/No)	Ufficio Affari Generali e Protocollo
denunce al Registro delle Imprese	Data, Numero di protocollo (assegnato in automatico dal sistema), Camera di Commercio di appartenza, Numero REA dell'impresa, C.F., Denominazione sociale.	Ufficio Registro Imprese
istanze (Ufficio Protesti)	Tipologia istanza (cancellazione, rettifica, riabilitazione, ecc), Nome e cognome (o denominazione sociale), numero Effetti, Importo (in automatico), tipo valori (contanti / cc), numero di registrazione (in automatico)	Ufficio Protesti
domanda di carta del conducente	1a emissione (Sì/No), Rinnovo (per scadenza / modifica dati), Sostituzione (Smarrimento /Furto /Malfunzionamento), Cambio Nazione, Dati Conducente (Cognome, Nome, CF, Luogo nascita, Data Nascita, Provincia, Sesso, Residenza, Dati Patente), Modalità di rilascio / consegna Carta	Ufficio Servizi Innovativi
domanda di carta di controllo	1a emissione (Sì/No), Rinnovo (per scadenza / modifica dati), Sostituzione (Smarrimento /Furto /Malfunzionamento), Cambio Nazione, Dati Organismo di Controllo (Denominazione, CF, Indirizzo, CAP, Comune, email), Dati del Responsabile (Cognome, Nome, CF), Modalità di rilascio / consegna Carta	Ufficio Servizi Innovativi
domanda di carta dell'azienda	1a emissione (Sì/No), Rinnovo (per scadenza / modifica dati), Sostituzione (Smarrimento /Furto /Malfunzionamento), Cambio Nazione, Dati Azienda (Denominazione, CF, Indirizzo, CAP, Comune, email), Dati del Titolare o legale rappresentante, Modalità di rilascio / consegna Carta	Ufficio Servizi Innovativi

domanda di carta dell'officina	1a emissione (Sì/No), Rinnovo (per scadenza / modifica dati), Sostituzione (Smarrimento /Furto /Malfunzionamento), Cambio Nazione, Dati dell'Unità Operativa autorizzata (Denominazione, CF, Num. autorizzazione, Indirizzo, CAP, Comune, email), Dati del Titolare o legale rappresentante, Attività svolte presso l'Officina, Modalità di rilascio / consegna Carta	Ufficio Servizi Innovativi
domande di marchio	Data, N. registrazione (fornito in automatico dal sistema), Anagrafica del richiedente (Nome e Cognome o denominazione sociale, C.F. / Partita IVA, Indirizzo, città)	Ufficio Innovazione
domande di brevetto	Data, N. registrazione (fornito in automatico dal sistema), Anagrafica del richiedente (Nome e Cognome o denominazione sociale, C.F. / Partita IVA, Indirizzo, città)	Ufficio Innovazione
modelli unici di dichiarazione ambientale	Denominazione, sede, CF, data presentazione	Ufficio Ambiente
richieste di certificato di origine	Numero progressivo e Data di registrazione, N. serie, Speditore, Destinatario, Luogo di rilascio, Data di rilascio, Quantità, Numero e Data Fattura, Numero ordine, Colli.	Ufficio Commercio Estero
richiesta di carnet ATA	Numero Carnet, Richiedente, Tipo richiedente, Indirizzo, Data rilascio, Utilizzo, Paese destinatario, Valore merce	Ufficio Commercio Estero
mandati / reversali	Numero progressivo, Fornitore, Numero fornitore, Conto bancario, Importo, Netto a pagare, Data Fattura, Descrizione, Anno approvazione, Data distinta, Numero distinta, Data riscontro	Ufficio Ragioneria
buoni d'ordine	Numero progressivo, Fornitore, Numero fornitore, Conto bancario, Importo, Netto a pagare, Data Fattura, Descrizione, Anno approvazione, Data distinta, Numero distinta, Data riscontro	Ufficio Provveditorato
ordini di servizio	Numero progressivo, Data	Ufficio Personale e Organizzazione