

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA DI GENOVA

Riunione della Giunta Camerale di lunedì 29 giugno 2026 - Ore 15.06

Presenti	Assenti		
☒	☐	Sig. Luigi ATTANASIO	- Presidente
☒	☐	Dott.ssa Barbara BANCHERO	
☐	☒	Sig.ra Maria Ornella CAMELLA	
☒	☐	Sig. Alessandro CAVO (*)	
☒	☐	Sig. Paolo CORSIGLIA	
☒	☐	Ing. Fabrizio FERRARI	
☐	☒	Dott. Felice NEGRI	
☒	☐	Sig. Massimiliano SPIGNO	
☒	☐	Dott. Massimiliano TUMIATI	- Presidente Revisori dei Conti
☒	☐	Dott. Gian Alberto MANGIANTE (**)	- Revisore dei Conti
☐	☒	Dott. Riccardo SCARPULLA	- Revisore dei Conti
☒	☐	Dott. Maurizio CAVIGLIA	- Segretario Generale

(*) Il sig. Cavo esce alle ore 16.01 durante la trattazione della delibera n. 297.

(**) Il dott. Mangiante esce alle ore 16.05 durante la trattazione della delibera n. 300.

Assistono il Segretario Generale il Dirigente Vicario, dott. Marco Razeto e la sig.ra Angela Modestini. Partecipano alla riunione il dott. Stefano Messina, in qualità di Presidente della Consulta per il settore marittimo, portuale e logistico, l'ing. Giulio Musso, in qualità di Presidente della Consulta per le infrastrutture e l'urbanistica.

N.295 del 29.06.2026

Oggetto: Aggiornamento del Manuale di gestione documentale.

Il PRESIDENTE riferisce:

Il DPCM 3 dicembre 2013, recante le "Regole tecniche per il protocollo informatico ai sensi degli artt.40 bis, 41, 47, 57 bis e 71 del Codice dell'Amministrazione Digitale di cui al D.Lgs. n.82 del 2005" ha disciplinato il contenuto del Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi, documento che "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi" (art.5).

La Giunta camerale con il provvedimento n.181 del 28.09.2015 ha deliberato l'approvazione del Manuale di Gestione documentale, aggiornato successivamente con i provvedimenti n.130 del 03.12.2018 e n.263 del 26.09.2022, anche per allinearne il contenuto alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici adottate dall'Agenzia per l'Italia Digitale con Determinazione n. 407/2020 e successive modificazioni e integrazioni.

Considerato che la normativa vigente e le Linee guida AgID prevedono che il Manuale sia costantemente aggiornato al fine di garantirne la coerenza con l'assetto organizzativo dell'Ente, con l'evoluzione normativa e con le modalità operative adottate, si ritiene necessario procedere ad un ulteriore aggiornamento del Manuale: il testo proposto in approvazione è riportato in allegato.

LA GIUNTA CAMERALE

Visto il decreto legislativo 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione Digitale" e successive modificazioni e integrazioni;

Visto il D.P.R. 28 dicembre 2000, n. 445 recante il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";

Viste le Linee guida sulla formazione, gestione e conservazione dei documenti informatici emanate dall'Agenzia per l'Italia Digitale (AgID) e i relativi aggiornamenti;

Richiamata la deliberazione della Giunta camerale n.181 del 28.09.2015 con la quale è stato adottato il Manuale di gestione documentale dell'Ente;

Richiamate le successive deliberazioni n.310 del 03.12.2018 e n.263 del 26.09.2022, con le quali si è proceduto all'aggiornamento del Manuale;

Considerato che il Manuale di gestione documentale costituisce lo strumento organizzativo di riferimento per la corretta formazione, gestione, protocollazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti dell'Ente;

Considerato che la normativa vigente e le Linee guida AgID prevedono che il Manuale sia costantemente aggiornato al fine di garantirne la coerenza con l'assetto organizzativo dell'Ente, con l'evoluzione normativa e con le modalità operative adottate;

Preso atto che, a seguito delle verifiche effettuate dagli uffici competenti, si è ritenuto opportuno procedere all'aggiornamento del Manuale al fine di recepire le intervenute modifiche normative, organizzative e procedurali e di assicurare l'allineamento alle attuali modalità di gestione documentale dell'Ente;

Vista la proposta di aggiornamento del Manuale di gestione documentale predisposta dal Responsabile della gestione documentale;

Unanime,

d e l i b e r a

- di approvare il "Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi" nella versione aggiornata, allegata alla presente deliberazione, di cui ne costituisce parte integrante;
- di autorizzare il Segretario Generale ad apportare con proprio provvedimento le variazioni agli allegati tecnici eventualmente necessarie a seguito di modifiche normative, organizzative oppure nel caso di acquisizione di nuove tecnologie.

ALLEGATO

Il Segretario Generale
f.to Dott. Maurizio Caviglia

Il Presidente
f.to Sig. Luigi Attanasio



Per copia conforme ad uso amministrativo
IL DIRIGENTE VICARIO
Dott. Marco RAZETO



Camera di Commercio
Genova



MANUALE DI GESTIONE DOCUMENTALE

(approvato con delibera n.295 del 29.06.2026)

SOMMARIO

1	PREMESSE	4
1.1	Riferimenti normativi	4
1.2	Glossario	6
1.3	Approvazione ed aggiornamento del Manuale	14
2	IL SISTEMA DI GESTIONE DOCUMENTALE	15
2.1	Aree Organizzative Omogenee	15
2.2	Il servizio per la tenuta del protocollo informatico	15
2.3	Ruoli e responsabilità	16
2.4	Il sistema di gestione documentale e protocollo informatico.	19
3	TUTELA DEI DATI PERSONALI E SICUREZZA DEL SISTEMA DI GESTIONE DOCUMENTALE	22
3.1	Accountability	22
3.2	Registro delle attività di trattamento di dati personali	22
3.3	Ruoli	22
3.4	Piano della sicurezza	23
3.5	Accessibilità al sistema di gestione e livelli di riservatezza	25
4	LA FORMAZIONE DEI DOCUMENTI	25
4.1	Modalità di formazione dei documenti e contenuti minimi	25
4.2	Firme elettroniche	26
4.3	Posta elettronica ordinaria	26
4.4	Posta elettronica certificata	26
4.5	I formati dei documenti informatici	27
4.6	I metadati dei documenti informatici	27
4.7	Sottoscrizione dei documenti informatici	29
4.8	La gestione dei documenti cartacei	29

4.9	Copie e duplicati	29
5	LA TRASMISSIONE DEI DOCUMENTI	31
5.1	Ricezione dei documenti informatici	31
5.2	Ricezione dei documenti su supporto cartaceo	31
5.3	Ricezione della posta elettronica ordinaria	32
5.4	Ricezione e gestione dei messaggi di posta elettronica certificata	32
5.5	Spedizione dei documenti cartacei	33
5.6	Spedizione dei documenti informatici	33
5.7	Domicilio digitale	33
5.8	Documenti interni	34
6	LA REGISTRAZIONE DEI DOCUMENTI	35
6.1	Documenti soggetti a registrazione di protocollo	35
6.2	Documenti non soggetti a registrazione obbligatoria di protocollo	35
6.3	Registrazione di protocollo dei documenti	36
6.4	Segnatura di protocollo	37
6.5	Annullamento e modifica delle registrazioni di protocollo	38
6.6	Differimento dei termini di registrazione	38
6.7	Registro giornaliero di protocollo	38
6.8	Registro annuale di protocollo	38
6.9	Registro di emergenza	38
7	CASI PARTICOLARI	41
7.1	Documentazione soggetta a registrazione particolare	41
7.2	Documentazione relativa a gare d'appalto	43
7.3	Documenti a carattere riservato, personale e/o confidenziale	43
7.4	Lettere anonime	43
7.5	Documenti non firmati o con firma illeggibile	43
7.6	Documentazione di competenza di altre amministrazioni o uffici	43

7.7	Documento inviato a più UO e/o pervenuto attraverso canali diversi	43
7.8	Oggetti plurimi	44
8	ASSEGNAZIONE E CLASSIFICAZIONE DEI DOCUMENTI	45
8.1	Assegnazione	45
8.2	Modifica delle assegnazioni	46
8.3	Consegna dei documenti cartacei	46
8.4	Consegna dei documenti informatici	47
8.5	Classificazione dei documenti	47
9	FASCICOLAZIONE DEI DOCUMENTI	48
9.1	Formazione dei fascicoli	48
9.2	Tipologie di fascicolo	49
9.3	Struttura gerarchica del fascicolo	50
9.4	Processo di identificazione e formazione dei fascicoli	52
9.5	Alimentazione dei fascicoli	53
9.6	Conservazione dei fascicoli	53
9.7	Gestione dello scarto	53
10	SCANSIONE DEI DOCUMENTI CARTACEI	55
10.1	Processo di scansione e certificazione di conformità	55
11	GESTIONE DOCUMENTI CARTACEI DEGLI ARCHIVI DI DEPOSITO	56
11.1	Gli archivi di deposito delle Unità organizzative (UO)	56
12	DISPOSIZIONI FINALI	65
	PIANO PER LA SICUREZZA INFORMATICA	62

1 Premesse

In ottemperanza a quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, la Camera di Commercio Industria e Artigianato di Genova ha redatto il presente Manuale di Gestione (MdG) con l'obiettivo di descrivere il sistema di gestione dei documenti, anche ai fini della conservazione, e di fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il Manuale di gestione è stato predisposto con una duplice finalità: da un lato disciplinare il sistema di gestione documentale dell'Ente e, dall'altro, rappresentare le funzionalità disponibili per tutti gli utenti, interni ed esterni, che interagiscono con la Camera di Commercio di Genova.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le indicazioni per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Pertanto, si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'ente.

In particolare, il Manuale disciplina:

- le modalità informatiche di formazione e scambio dei documenti dell'amministrazione e la loro gestione;
- la gestione dei flussi documentali
- l'utilizzo del sistema di gestione documentale
- l'uso del Titolario e del Piano di fascicolazione
- la conservazione dei documenti
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo o interesse.
- le politiche di protezione dati e il Piano della sicurezza

Il presente manuale è pubblicato sul sito internet istituzionale della Camera di Commercio, all'interno della Sezione "Amministrazione trasparente" nella sottosezione "Disposizioni Generali > Atti generali".

1.1 Riferimenti normativi

La normativa di riferimento per la gestione dei documenti informatici all'interno della pubblica amministrazione è rappresentata da:

- **Codice dei Beni Culturali e del paesaggio:** il decreto legislativo 22 gennaio 2004, n. 42.
- **Codice dell'Amministrazione digitale:** il decreto legislativo 7 marzo 2005, n. 82 – CAD.
- **Legge sul procedimento:** la Legge 7 agosto 1990, n. 241 – Legge sul procedimento amministrativo.
- **Testo unico della documentazione amministrativa:** il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa – TUDA.

- **Codice Privacy:** il decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali.
- **GDPR – Regolamento (UE) n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (General Data Protection Regulation),** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- **Decreto Trasparenza:** il decreto legislativo 14 marzo 2013, n. 33 – Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle pubbliche amministrazioni.
- **Decreto legislativo 25 maggio 2016, n. 97 (FOIA)** - Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza.
- **Circolare del Ministro per la semplificazione e la pubblica amministrazione n. 2/2017** - Attuazione delle norme sull'accesso civico generalizzato (FOIA).
- **Decreto legislativo 19 agosto 2005 n. 195** - Attuazione della direttiva 2003/4/CE sull'accesso del pubblico all'informazione ambientale.
- **Linee Guida ANAC** - Delibera n. 1309/2016 - Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del D.Lgs. 33/2013.
- **Codice dei Contratti Pubblici:** il Decreto legislativo 31 marzo 2023, n. 36 – Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici.
- **Linee Guida** sulla formazione, gestione e conservazione dei documenti informatici.
- **Legge sull'accessibilità:** la Legge 9 gennaio 2004, n. 4 – Disposizioni per favorire l'accesso dei disabili agli strumenti informatici.
- **Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014:** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - art. 21, comma 5, del decreto legislativo n. 82/2005. Circolare dell'Agenzia per l'Italia Digitale - AgID 10 aprile 2014, n. 65.
- **Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55:** Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della Legge 24 dicembre 2007, n. 244.
- **Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68:** Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della Legge 16 gennaio 2003, n. 3.
- **Decreto Legislativo 5 agosto 2015, n. 127:** Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'art. 9, comma 1, lettere d) e g), della Legge 11 marzo 2014, n. 23.

- **Decreto del Presidente del Consiglio dei ministri del 10 dicembre 2008:** Specifiche tecniche del formato elettronico elaborabile (XBRL) per la presentazione dei bilanci di esercizio e consolidati e di altri atti al registro delle imprese.
- **Circolare del Ministro per la pubblica amministrazione del 1° ottobre 2018 n. 3:** Responsabile per la transizione digitale - art. 17 decreto legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale”
- **Regolamento eIDAS:** il Regolamento (UE) No 910/2014 del 23 luglio 2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- **Linee Guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate,** emanate con Determinazione AgID No 121/2019.
- **Regole tecniche per le firme elettroniche:** il decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 recante “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”.
- **Regole tecniche per il protocollo:** il decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, recante “Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell’Amministrazione digitale di cui al decreto legislativo n. 82”, così come modificato dal decreto legislativo 26 agosto 2016, n. 179.
- **Piano Triennale per l’informatica nella Pubblica Amministrazione 2024-2026** (o semplicemente Piano Triennale): lo strumento essenziale per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione italiana.

In materia di sicurezza informatica, la Camera di Commercio di Genova si conforma inoltre alle indicazioni tecniche emanate dall’Agenzia per la Cybersicurezza Nazionale (ACN), istituita con D.L. 14 giugno 2021, n. 82, convertito con L. 4 agosto 2021, n. 109. In particolare, recepisce le misure e le linee guida emanate dall’ACN per la PA, ivi incluse quelle relative alla classificazione dei dati e alla sicurezza dei servizi cloud.

1.2 Glossario

Ai fini del presente documento si intendono:

- **Accesso**, operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti amministrativi informatici
- **Accreditamento**, riconoscimento, da parte dell’Agenzia per l’Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
- **Affare**, complesso di documenti prodotti (spediti, ricevuti, allegati, ecc.) da un ente, relativi alla trattazione di un

oggetto specifico di sua competenza; si chiama affare o anche pratica.

- **Allegato**, documento unito a un documento o a una pratica per prova, per chiarimento o integrazione di notizie, per memoria.
- **Archivio**, il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività. Con questo termine si intende anche il luogo fisico di conservazione della documentazione
- **Archivio informatico**, archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
- **Area Organizzativa Omogenea (AOO)**, insieme di funzioni e di strutture che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del Testo Unico.
- **Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico**, dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
- **Autenticità**, caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
- **Classificazione**, strumento per la formazione dell'archivio, cioè per l'ordinamento di tutti i documenti prodotti e acquisiti nello svolgimento dell'attività amministrativa.
- **Conservatore accreditato**, soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
- **Conservazione**, insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
- **Copia analogica del documento informatico**, documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
- **Dato personale**, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1 del GDPR).
- **Delegati**, personale dell'ente incaricato formalmente dal RGD per l'espletamento di funzioni previste dal presente Manuale.

- **Destinatario**, identifica il soggetto/sistema al quale il documento informatico è indirizzato
- **Documento informatico**: rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti (art. 1 comma 1 lett. p) del CAD)
- **Documento analogico**: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. p bis) del CAD)
- **Domicilio digitale**, un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito «Regolamento eIDAS», valido ai fini delle comunicazioni elettroniche aventi valore legale
- **Duplicazione dei documenti informatici**, produzione di duplicati informatici
- **Esibizione**, operazione che consente di visualizzare un documento conservato e di ottenerne copia
- **Evidenza informatica**, una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
- **Fascicolo informatico**, Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD.
- **firma elettronica**, insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- **Firma elettronica avanzata**, insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
- **Firma digitale**, è un particolare di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica una privata, 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; firma elettronica, ai sensi dell'articolo 2, comma 1, lettera g, del decreto legislativo 10/2002, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.
- **Formato contenitore**, formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
- **Formato del documento informatico**, modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

- **Flusso documentale**, movimento dei documenti all'interno dell'archivio (dalla fase di formazione dell'archivio corrente a quella di conservazione dell'archivio storico).
- **Funzione di hash**, una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.
- **GEDOC – Sistema di gestione documentale** (GEDOC), sistema informatico utilizzato per la protocollazione dei documenti in ingresso e uscita, la classificazione secondo un Titolario, la fascicolazione e l'archiviazione dei documenti di rilevanza amministrativa.
- **Gestione dei documenti**, l'insieme di attività finalizzate alla registrazione di protocollo e alla classificazione, fascicolazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato (Piano di classificazione)
- **Identificazione informatica**, la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco a un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso
- **Identificativo univoco**, sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione;
- **Interoperabilità**, caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
- **Immodificabilità**, caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso;
- **Impronta**, la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash. Un'evidenza informatica di lunghezza predefinita ottenuta da un'altra evidenza informatica mediante un'opportuna funzione matematica tale che risulti di fatto impossibile, a partire dall'impronta, ricostruire l'evidenza informatica che l'ha generata, ed altresì risulti di fatto impossibile determinare una coppia di evidenze informatiche per le quali la funzione generi impronte uguali.
- **Interoperabilità**, possibilità di trattamento automatico, da parte del sistema di protocollo ricevente, delle informazioni trasmesse dal sistema di protocollo mittente, allo scopo di automatizzare le attività e i procedimenti amministrativi conseguenti.
- **Leggibilità**, insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;
- **Log di sistema**, registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di

controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati;

- **Manuale di Gestione del protocollo informatico, dei documenti e degli archivi (MdG)**, strumento che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
- **Massimario di selezione** anche detto di scarto, il massimario di selezione è lo strumento che consente di coordinare razionalmente lo scarto archivistico (cioè la destinazione al macero) dei documenti prodotti dagli enti pubblici e dagli organi centrali e periferici dello Stato. Il massimario riproduce l'elenco delle partizioni (categorie) e sottopartizioni del Titolare con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo trent'anni dall'esaurimento degli affari nei competenti Archivi di Stato) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc.
- **Metadati**, insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione;
- **Oggetto**, in sede di formazione del documento l'oggetto è l'enunciazione sommaria, sintetizzata in poche parole, al massimo un paio di righe, dell'argomento di cui tratta il documento. L'oggetto viene scritto sul documento nello spazio apposito e deve essere riportato (talora con parole diverse) sia sul registro di protocollo dell'ente che scrive sia su quello dell'ente che riceve il documento.
- **Pacchetto di versamento (PdV)**, pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
- **Piano di conservazione**, piano di conservazione, documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
- **Piano di Classificazione**, sistema precostituito e stabile, individuato sulla base delle funzioni dell'ente, al quale devono essere ricondotti i documenti prodotti
- **Piano della sicurezza del sistema di gestione informatica dei documenti**, documento che descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza;
- **Posta elettronica certificata (PEC)**, sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
- **Posta elettronica ordinaria (PEO)**, sistema di comunicazione che non attesta l'invio e l'avvenuta consegna di un messaggio di posta elettronica e non fornisce ricevute opponibili ai terzi;
- **Pubblico ufficiale**, il notaio, salvo quanto previsto dall'art. 5, comma 4 della presente deliberazione e nei casi per i

quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2 del DPR 445/2000.

- **Registrazione di protocollo**, attività che permette di identificare in modo certo i documenti ricevuti o spediti su qualunque supporto di trasmissione da un soggetto produttore; ha una finalità giuridico-probatoria ed è strumento di certificazione e di verifica dell'autenticità dei documenti;
- **Registro**, unità archivistica costituita da un insieme di fogli rilegati. Nel registro vengono trascritti o registrati per esteso o per sunto documenti e minute di documenti, ovvero vengono effettuate trascrizioni, registrazioni e annotazioni costitutive dell'atto giuridico. Spesso si usa impropriamente l'espressione volume come sinonimo di registro;
- **Registro particolare**, registro informatico, regolato da norme specifiche, usato per particolari tipologie documentali e che può contenere trascrizioni, registrazioni e annotazioni costitutive di un atto giuridico, previsto ai sensi dell'articolo 53, comma 5 del DPR 445/2000;
- **Registro di protocollo**, registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti;
- **Repertorio informatico**, registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;
- **Repertorio della Serie**, registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del Titolario: il repertorio deve essere organizzato in maniera da riprodurre le suddivisioni del Titolario;
- **Responsabile del Procedimento (RdP)**, il dipendente che assume su di sé la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un singolo procedimento amministrativo;
- **Responsabile della gestione documentale (RGD)**, ovvero Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali, nonché degli archivi;
- **Responsabile della Conservazione**, dirigente o funzionario formalmente designato che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;
- **Responsabile della protezione dei dati**, il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Reg. UE 2016/679. Trattasi di un dipendente del titolare del trattamento o del responsabile del trattamento oppure di un incaricato all'assolvimento dei suoi compiti sulla base di un contratto di servizi (art. 37 del Reg. UE 2016/679);
- **Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi**, dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico

archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione;

- **Responsabile del trattamento dei dati**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **Responsabile della Transizione al Digitale**, figura dirigenziale all'interno della PA che ha tra le sue principali funzioni quella di garantire operativamente la trasformazione digitale dell'amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di nuovi modelli di relazione trasparenti e aperti con i cittadini;
- **Responsabile della sicurezza**, soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza);
- **Riferimento temporale**, informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
- **Scarto**, operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale;
- **Segnatura di protocollo**, apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni che consentono di identificare/individuare in modo inequivocabile il documento stesso;
- **Serie archivistica**, ciascun raggruppamento di documenti con caratteristiche omogenee, all'interno di un fondo archivistico. Può essere articolata in sottoserie;
- **Servizio archivistico**, il servizio per la gestione dei documenti, del protocollo, dei flussi documentali e degli archivi analogici e informatici;
- **Sistema informativo**, insieme degli strumenti e procedure che consente l'accesso sul web alle risorse archivistiche e ne permette la gestione e fruibilità;
- **Sistema di gestione informatica dei documenti**, nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445;
- **Sistema di conservazione**, sistema di conservazione dei documenti informatici di cui all'art. 44 del CAD;
- **Sottofascicolo**, articolazione interna al fascicolo;
- **Titolare del trattamento dei dati**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **Titolario di classificazione**, sistema precostituito di schemi di voci gerarchicamente ordinate, individuato in base alle

funzioni e alle materie di competenza dell'amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la conservazione secondo un ordine logico. Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato;

- **Trasmissione telematica**, trasmissione di documenti attraverso servizi di telecomunicazione;
- **Trattamento dei dati**, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Utente**, persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse;
- **Unità archivistica**, termine generico con cui si individua l'unità minima indivisibile di un fondo archivistico, che può aggregare più documenti, fisicamente contigui, o essere costituita da una singola unità documentaria. Può essere costituita da un fascicolo, un registro, una filza, un volume ecc.
- **Unità Organizzativa (UO)**: ufficio che, per tipologia di funzioni e di competenza, presenta esigenze di gestione della documentazione unitarie e coordinate;
- **Validazione temporale**, il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;
- **Vicario**, il dipendente che assume le funzioni e i compiti del Responsabile della gestione documentale nei casi di assenza, vacanza o impedimento di quest'ultimo;
- **Vigilanza**, Indica l'insieme delle funzioni attribuite alle Soprintendenze archivistiche relative alla tutela degli archivi degli enti pubblici, territoriali e non territoriali, e degli archivi privati, conservati di massima presso l'ente produttore o presso istituzioni culturali diverse dagli Archivi di Stato;
- **Vincolo archivistico**, nesso che collega in maniera logica e necessaria i documenti che compongono l'archivio di un ente;
- **Violazione dei dati personali**, la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

1.3 Approvazione ed aggiornamento del Manuale

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è stato adottato con delibera della Giunta Camerale ed è stato pubblicato sul sito istituzionale nell'area "Amministrazione trasparente" prevista dall'art. 9 del D.Lgs. n.33/2013. Esso descrive il sistema di gestione dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e dell'archivio corrente. È redatto a cura del Responsabile della gestione documentale (RGD), che ne propone lo schema alla Giunta Camerale.

Il Manuale, in un contesto di continua trasformazione, deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e strumenti utilizzati. Allo stesso modo anche i processi e le attività inerenti alle attività di formazione dei documenti devono essere sottoposti a costante valutazione e monitoraggio. Il RGD provvederà alle eventuali integrazioni o revisioni nei casi in cui lo ritenga opportuno, ad esempio a seguito di:

- modifiche normative o regolamentari sopravvenute;
- introduzione di nuove pratiche tendenti a migliorare l'operatività dell'ente in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- sostanziali modifiche apportate nell'ambito dell'architettura del sistema e delle singole componenti informatiche utilizzate.

In caso ritenga necessario apportare aggiornamenti, il RGD li propone alla Giunta Camerale fornendo ogni informazione utile all'assunzione della relativa deliberazione. Gli allegati del presente documento possono essere modificati con atto unilaterale del Responsabile della Gestione Documentale; la modifica acquista efficacia al momento della pubblicazione sul sito web dell'amministrazione.

Nel caso di avvicendamento del RGD, il nuovo Responsabile deve prendere visione del manuale di gestione, verificare le regole in esso contenute ed eventualmente modificarle, proponendo aggiornamenti del manuale stesso.

2 Il Sistema di Gestione documentale

2.1 Aree Organizzative Omogenee

L'ente ha scelto di configurarsi, ai fini della gestione documentale, come unica Area Organizzativa Omogenea (di seguito AOO), composta dall'insieme di unità organizzative articolate come riportato nell'allegato 1 (cd *"funzionigramma"*) e di definire, quindi, un unico sistema di gestione documentale e protocollo informatico.

I vantaggi derivanti da tale scelta organizzativa sono i seguenti:

- omogeneità di organizzazione del servizio
- riduzione dei costi di gestione del servizio
- eliminazione della frammentazione dei sistemi di protocollo
- maggiore flessibilità del servizio
- indipendenza dalle dinamiche di riorganizzazione dell'ente
- semplificazione delle operazioni di archiviazione e reperimento dei documenti
- riduzione della ridondanza della documentazione da gestire
- semplificazione dell'iter documentale.

Per la protocollazione dei documenti in entrata si è adottato un modello operativo di tipo centralizzato presso l'Ufficio di protocollo generale (Ufficio Affari Generali e Protocollo). Per la protocollazione dei documenti in uscita si è adottato invece un modello decentralizzato presso ciascuna Unità Organizzativa (UO).

2.2 Il servizio per la tenuta del protocollo informatico

Ai sensi dell'art. 61.1 del DPR 28 dicembre 2000 n. 445 - T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - la Camera di Commercio Industria Artigianato e Agricoltura di Genova ha provveduto ad istituire uno specifico ed unitario Servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi e, ai sensi dell'art. 61.2 del suddetto T.U.

Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi è istituito nella AOO.

2.3 Ruoli e responsabilità

Nel sistema di gestione documentale sono stati individuati i seguenti ruoli previsti dalla normativa vigente:

Responsabile della gestione documentale	Art. 61 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Disposizioni legislative in materia di documentazione amministrativa
Responsabile della conservazione	Art. 44 del decreto legislativo 7 marzo 2005, n. 82
Responsabile della transizione al digitale	Art. 17 del Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale Circolare n. 3 del 1° ottobre 2018 del Ministro per la pubblica amministrazione
Responsabile della protezione dei dati	Art. 37 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Il Responsabile della gestione documentale

La Camera di Commercio Industria Artigianato e Agricoltura di Genova, nel rispetto della normativa vigente, ha conferito, con delibera n.221 del 1° luglio 2019 al dott. Marco Razeto il ruolo di responsabile del “servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi” (Responsabile della gestione documentale).

Al Responsabile, sulla base di quanto previsto dalla normativa spetta il compito di:

- predisporre lo schema del Manuale di gestione;
- verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.
- predisporre il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:
 - o misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
 - o disposizioni in materia di protezione dei dati personali;
 - o indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.
- curare la formazione del personale in materia di gestione documentale e rendere disponibile tutta la documentazione relativa all'uso dell'hardware e software in uso all'ente (es. manuali d'uso)
- provvedere a generare, per uno o più documenti informatici, un pacchetto di versamento nelle modalità e con i formati concordati con il responsabile della conservazione e previsti dal manuale di conservazione e, in quanto produttore del Pacchetto di Versamento (PdV), verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

Al Responsabile della gestione documentale spetta, altresì, l'invio periodico all'archivio di deposito e/o al sistema di conservazione dei fascicoli e delle serie documentarie relative a procedimenti anche non conclusi, e l'elaborazione e aggiornamento del Piano di conservazione dei documenti, siano essi digitali o cartacei. Per i casi di vacanza, assenza o impedimento del RGD è stato nominato, quale vicario, il dott. Maurizio Floris, il quale è stato delegato alla firma dei registri giornalieri ed annuali di protocollo e alla loro trasmissione, entro la giornata lavorativa, al sistema di conservazione.

Responsabile della conservazione

Il Responsabile della conservazione della Camera di Commercio Industria Artigianato e Agricoltura di Genova è il dott. Maurizio Floris, nominato con determinazione del Segretario Generale n.293 del 2 agosto 2016.

Il Responsabile della conservazione è la persona incaricata di curare l'insieme delle attività finalizzate alla conservazione dei documenti. In virtù della trasversalità delle sue funzioni, il responsabile si avvale della collaborazione del Responsabile del trattamento dei dati personali, del Responsabile della sicurezza, del Responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali coincide con il responsabile dell'ufficio di cui all'art. 17 del CAD (Responsabile della transizione al digitale), e del Responsabile della gestione documentale.

Al Responsabile della conservazione compete l'insieme delle seguenti attività descritte nelle Linee Guida Agid:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

- provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali
- predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il responsabile della conservazione può affidare, in tutto o in parte, lo svolgimento del processo di conservazione a un conservatore accreditato da Agid, ai sensi dell'art. 44 del CAD. Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Attraverso un'apposita convenzione per l'affidamento del servizio di conservazione a norma dei documenti informatici (art. 5, c.3 delle Regole Tecniche), la Camera di Commercio ha affidato a InfoCamere, società consortile delle CCIAA e soggetto conservatore accreditato presso Agid, alcune parti del processo di conservazione.

Responsabile della transizione al digitale

Con delibera di Giunta n.126 del 26 aprile 2021 il ruolo di Responsabile della transizione al digitale è stato conferito al dott. Maurizio Caviglia. Le funzioni del Responsabile della transizione al digitale sono elencate dal comma 1 dall'articolo 17 del CAD, che attribuisce all'Ufficio per la transizione digitale i compiti relativi a:

- coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
- indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
- accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità;
- analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- cooperazione alla revisione della riorganizzazione dell'amministrazione;
- indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei

ministri o dal Ministro delegato per l'innovazione e le tecnologie;

- pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;
- pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale.

Il Responsabile della Protezione dei Dati (DPO)

Il Responsabile della Protezione dei Dati è designato ai sensi dell'art. 37 del Regolamento (UE) 2016/679 (GDPR). Con delibera n. 123 del 07.05.2018 la Giunta camerale ha nominato il dott. Maurizio Floris.

Nell'ambito del sistema di gestione documentale, il DPO svolge le seguenti funzioni:

- esprime parere obbligatorio sulla predisposizione e l'aggiornamento del Piano della sicurezza del sistema di gestione informatica dei documenti (par. 3.4), con particolare riferimento alle misure a protezione dei dati personali trattati attraverso il sistema GEDOC;
- partecipa alla valutazione d'impatto sulla protezione dei dati (DPIA) ogniqualvolta l'introduzione o la modifica del sistema di gestione documentale possa comportare un rischio elevato per i diritti e le libertà degli interessati, ai sensi dell'art. 35 GDPR;
- verifica la coerenza tra i tempi di conservazione dei documenti stabiliti nel Piano di conservazione e i principi di limitazione della conservazione di cui all'art. 5, par. 1, lett. e) GDPR;
- supervisiona la corretta applicazione dei livelli di riservatezza e delle misure di controllo dell'accesso al sistema GEDOC in relazione ai documenti contenenti dati personali;
- collabora con il Responsabile della gestione documentale nella definizione delle procedure per la gestione delle violazioni dei dati personali (data breach) che coinvolgano la documentazione archiviata nel sistema.

Il DPO agisce in piena indipendenza funzionale e riferisce direttamente al vertice dell'ente.

2.4 Il sistema di gestione documentale e protocollo informatico.

L'art. 1 comma 1 lettera r) del Dpr 445 del 2000 definisce il Sistema di gestione informatica dei documenti come: "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti". La Camera utilizza il sistema di protocollo informatico "**GEDOC – Nuovo sistema di gestione documentale**" (in breve GEDOC) realizzato e fornito da Infocamere Scpa nell'ambito dei rapporti in essere con l'amministrazione.

Il Sistema è integrato con gli strumenti di gestione documentale quali: il Titolario, il Piano di fascicolazione e il Piano di conservazione, descritti negli allegati al presente documento.

GEDOC si interfaccia con gli applicativi usati dall'amministrazione per la gestione di determinati processi e/o procedimenti e garantisce che le operazioni di registrazione, archiviazione e invio in conservazione della documentazione prodotta si svolgano nel rispetto della normativa vigente e delle regole riportate negli strumenti di gestione documentale adottati.

Il sistema GEDOC, le risorse strumentali e le procedure utilizzate dalla Camera di Commercio per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento nell'ambito dell'AOO;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo.

In GEDOC non viene gestita la documentazione soggetta a registrazione particolare (vedi par. 7.1).

3 Tutela dei dati personali e sicurezza del sistema di gestione documentale

Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, noto come GDPR (General Data Protection Regulation), e che abroga la direttiva 95/46/CE, impone ai Titolari del trattamento di mettere in atto misure di sicurezza tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia svolto nel rispetto delle previsioni legislative europee e nazionali, nonché per tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

3.1 Accountability

I Titolari e i Responsabili del trattamento sono tenuti a mettere in atto misure adeguate ed efficaci per la tutela dei dati personali e devono essere in grado di dimostrare la conformità alla disciplina in materia di dati personali delle attività svolte e l'efficacia e l'adeguatezza delle misure concretamente adottate.

In particolare, il Titolare del Trattamento deve essere in grado di dimostrare che le attività di trattamento svolte rispondano ai principi di liceità dettati dall'art. 5 GDPR, ossia che i dati siano:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, par. 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Affinché i dati siano trattati in modo lecito, il trattamento deve essere fondato su almeno uno dei legittimi presupposti (basi giuridiche) elencati dall'art.6 GDPR per quanto concerne i dati personali c.d. "comuni" (a titolo d'esempio, dati anagrafici e dati di contatto), all'art. 9 per le categorie particolari di dati e all'art. 10 per i dati relativi a condanne penali e reati. Con riferimento alle categorie particolari di dati personali, nonché ai dati relativi a condanne penali e reati, al

fine di individuare compiutamente la corretta base giuridica, deve tenersi conto, altresì, della disciplina nazionale in materia di protezione dei dati personali, contenuta negli artt. 2-sexies, 2-septies e 2-octies D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018.

Per quanto concerne poi, i trattamenti ulteriori svolti per finalità di archiviazione nel pubblico interesse, condizione essenziale per la liceità e correttezza degli stessi è il rispetto delle regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica, di cui al Provvedimento n. 513 del 19 dicembre 2018 Garante Privacy, pubblicate in G.U. n. 12 del 15 gennaio 2019.

Per la definizione dei tempi massimi di conservazione (c.d. *data retention*), sia che il trattamento avvenga con modalità cartacee sia che avvenga con modalità digitali, la Camera ha fatto riferimento alle tempistiche riportate nel Piano di conservazione delle Camere di Commercio, di cui all'art. 68 del Dpr 445/2000, fatto salvo l'ulteriore lasso di tempo necessario per completare le operazioni richieste dal procedimento di selezione e scarto archivistico.

I dati possono essere trattati per periodi ulteriori unicamente per finalità di archiviazione nel pubblico interesse conformemente a quanto previsto dall'art. 89, par. 1, GDPR e delle norme del Codice dei Beni Culturali (artt. 122 – 127 T.U. 42/2004). I documenti sono conservati nell'archivio nel rispetto delle misure tecniche e organizzative previste dalla normativa a tutela dei diritti e delle libertà dell'interessato.

3.2 Registro delle attività di trattamento di dati personali

Strettamente correlato al principio di *accountability*, e indispensabile a tal fine, è l'obbligo imposto dall'art. 30 GDPR in ordine alla tenuta e all'aggiornamento del Registro delle attività di trattamento, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminarmente rispetto a tali attività.

I contenuti minimi del Registro previsti dall'art. 30 GDPR sono il nome e i dati di contatto del titolare del trattamento, le finalità del trattamento (e la base giuridica per ciascuna finalità), una descrizione delle categorie di interessati e delle categorie di dati personali, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Registro delle attività di trattamento è stato adottato con delibera n.71 del 25 febbraio 2019, e successivamente aggiornato periodicamente. Il Registro contiene, oltre agli elementi fondamentali indicati dall'art. 30 GDPR, ulteriori elementi di dettaglio e descrittivi indispensabili, in ottica di *accountability*, all'Ente per documentare ed argomentare coerentemente le proprie scelte ed essere così in grado di dimostrare di aver operato correttamente.

3.3 Ruoli

Alla luce del principio di "responsabilizzazione", la Camera è tenuta a definire, nell'ambito della propria struttura organizzativa interna, i compiti e responsabilità in capo ai soggetti comunque coinvolti nei processi di trattamento di dati personali quali: soggetti designati/autorizzati, referenti, amministratori di sistema interni. Nella definizione dei compiti e delle responsabilità interne, e dunque nel conferimento delle designazioni / autorizzazioni al trattamento di dati personali, occorre prestare la massima attenzione all'assegnazione dei poteri di accesso, inserimento, modifica,

eliminazione (etc.) dei dati trattati dall'Ente, al solo personale che necessita effettivamente di effettuare tali operazioni in ragione dello svolgimento delle proprie mansioni. A tal fine la Camera di Commercio ha adottato un proprio modello organizzativo Privacy con la delibera n.222 del 1° luglio 2019.

3.4 Piano della sicurezza

Il Responsabile della gestione documentale predispone, in accordo con il Responsabile della conservazione, il Responsabile dell'ufficio per la transizione al digitale e acquisito il parere del Responsabile della protezione dei dati personali, il Piano della sicurezza del sistema di gestione informatica dei documenti, nel rispetto delle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017.

In materia di sicurezza informatica, la Camera si conforma inoltre alle indicazioni tecniche emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN), istituita con D.L. 14 giugno 2021, n. 82, convertito con L. 4 agosto 2021, n. 109. In particolare:

- adotta il Framework Nazionale per la Cybersecurity e la Data Protection come riferimento metodologico per la valutazione e la gestione del rischio informatico;
- recepisce le misure e le linee guida emanate dall'ACN per le pubbliche amministrazioni, ivi incluse quelle relative alla classificazione dei dati e alla sicurezza dei servizi cloud;
- verifica periodicamente l'adesione ai requisiti minimi previsti dalla normativa vigente, anche attraverso l'adozione di piani di adeguamento progressivo.

Il Piano della sicurezza del sistema di gestione informatica dei documenti viene aggiornato periodicamente dall'Ente e garantisce che:

- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, particolari e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Le misure di sicurezza garantiscono che:

- le informazioni e i dati siano disponibili, integri e protetti secondo il loro livello di riservatezza;
- per i documenti e i fascicoli informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale e l'estensione della validità temporale;
- gli atti, i documenti e i dati, in relazione alle conoscenze acquisite in base all'evoluzione tecnologica, alla loro natura e alle specifiche caratteristiche del trattamento, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta e della gestione;

Le misure generali tecniche e organizzative inerenti alla gestione documentale sono le seguenti:

- analisi del rischio

- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di una credenziale di identificazione interna (utente), di una credenziale riservata di autenticazione (password) e di un profilo di accesso;
- cambio delle password con frequenza stabilita nel Piano della sicurezza;
- gestione delle postazioni individuali e mantenimento della scrivania e schermo puliti (mediante apposita *"Clear desk and clear screen policy"*);
- gestione, dismissione e smaltimento degli apparati mobili e dei supporti;
- gestione del servizio con particolare riferimento sia all'esecuzione, che alla gestione delle copie di back-up dei dati e dei documenti da effettuarsi con frequenza giornaliera;
- impiego e manutenzione di un adeguato sistema antivirus;
- tracciamento delle attività nel file di log del sistema;
- monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

3.5 Accessibilità al sistema di gestione e livelli di riservatezza

Il sistema di gestione documentale è organizzato nel rispetto delle norme vigenti in materia di diritto di accesso (artt. 22 e ss. L. 241/1990 sul procedimento amministrativo e D.Lgs. n. 33/2013 sulla Trasparenza) e protezione dei dati personali (D. Lgs n. 196/2003 e GDPR). I dipendenti della camera di Commercio possono legittimamente accedere soltanto alle informazioni, ai documenti e ai fascicoli presenti nel sistema, la cui consultazione sia relativa a procedimenti e attività di propria competenza, ovvero secondo la posizione che rivestono all'interno del *funzionigramma* della Camera. Ciascun dipendente dell'amministrazione è in possesso di credenziali di accesso, consegnate previa identificazione dei soggetti stessi, in modo da creare un'associazione univoca tra identità fisica e identità digitale. Sulla base delle funzioni svolte sono assegnate le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate dal sistema. Il sistema di gestione documentale consente il controllo differenziato dell'accesso alle risorse di sistema per ciascun utente o gruppi di utenti, permettendo altresì di tracciare tutte le operazioni svolte individuandone, all'occorrenza, l'autore.

I profili di accesso al sistema sono suddivisi secondo le seguenti categorie:

- Responsabile della gestione documentale e addetti all'Ufficio Protocollo, che hanno la visibilità completa di tutti gli oggetti documentali del sistema, quali: schede, documenti, allegati, fascicoli, registri, etc.
- Utente, che ha la visibilità per competenza o per conoscenza delle schede documentali e dei fascicoli secondo il *funzionigramma*.

4 La formazione dei documenti

Per documento amministrativo si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Ciò premesso, il documento amministrativo va distinto in:

- documento analogico
- documento informatico

Tutti i documenti originali, indipendentemente dal loro supporto, sono tra loro connessi da speciale vincolo originario (vincolo archivistico), necessario e determinato e costituiscono l'archivio della Camera.

Ogni documento amministrativo è riferito ad un solo protocollo e può fare riferimento ad uno o più fascicoli.

4.1 Modalità di formazione dei documenti e contenuti minimi

La Camera di Commercio forma gli originali dei propri atti come documenti informatici, ai sensi dell'art. 40, comma 1 del CAD, o come copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico, consistenti nella scansione di ogni singola unità documentale pervenuta in via analogica. La loro esibizione e produzione sostituisce quella dell'originale e hanno piena efficacia ai sensi degli articoli 2714 e 2715 del Codice civile, se formati ai sensi dell'articolo 20, comma 1-bis del D.lgs. 82/2005.

In particolare, i documenti informatici sono formati secondo le seguenti principali modalità:

- Redazione tramite l'utilizzo di appositi strumenti software (Word di Microsoft Office)
- Acquisizione per via telematica o su supporto informatico di documenti informatici
- Acquisizione della copia per immagine su supporto informatico di un documento analogico
- Acquisizione della copia informatica di un documento analogico
- Registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari
- 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.

In particolare, riguardo la prima modalità sono previsti dei modelli di riferimento per la redazione della documentazione, resi disponibili ai dipendenti sulla rete intranet "Teams", che stabiliscono il "layout" (compreso i font). L'utilizzo dei modelli di riferimento e il rispetto di apposite linee guida assicurano la formazione dei documenti prodotti dall'amministrazione in conformità alla normativa in materia di accessibilità (Legge n. 4/2004 e relative disposizioni di attuazione).

Gli originali riportano, ove disponibili, le seguenti informazioni:

- logo e denominazione completa dell'amministrazione;
- indicazione dell'UO mittente;
- data del documento;

- dati del destinatario o dei destinatari (recapito di posta elettronica certificata o ordinaria, recapito fisico);
- oggetto del documento;
- testo del documento;
- numero e descrizione degli eventuali allegati;
- dati dell'Ente (indirizzo completo, numeri di telefono, indirizzi PEC o PEO a cui indirizzare risposta);

Sono incaricati della verifica della presenza delle seguenti informazioni sia il personale coinvolto nella redazione del documento che il personale addetto alle funzioni di protocollo;

I documenti dell'AOO sono prodotti con l'ausilio di applicativi che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

All'atto del caricamento del documento nel sistema di gestione documentale è previsto l'inserimento almeno di un set minimo di metadati richiesti obbligatoriamente dal sistema.

4.2 Firme elettroniche

La Camera di Commercio Industria Artigianato e Agricoltura di Genova fornisce la firma digitale ai soggetti da essa delegati a rappresentarla per l'espletamento delle attività istituzionali, per quelle relative ai processi, funzioni e atti amministrativi, nonché per le attività connesse all'attuazione della normativa relativa alla gestione dei documenti informatici.

4.3 Posta elettronica ordinaria

Il servizio di posta elettronica è disponibile per tutti gli utenti dell'Ente che vengono dotati di una casella di posta elettronica e che accedono utilizzando il proprio account utente di dominio (con relativa login e password). Per i dipendenti, l'indirizzo di posta elettronica è costituito dall'account utente di dominio con l'aggiunta del suffisso "@ge.camcom.it". Inoltre, vengono utilizzate caselle di servizio funzionali all'attività lavorativa delle singole strutture. Per le attività di registrazione di protocollo di documenti provenienti dall'esterno che erroneamente vengano indirizzate su caselle di PEO della Camera di Commercio è prevista la trasmissione alla casella di posta elettronica Protocollo@ge.camcom.it destinata a raccogliere e-mail con documenti ed eventuali allegati da protocollare. Le modalità di trasmissione sono descritte nel paragrafo 5.3.

4.4 Posta elettronica certificata

L'ente utilizza la PEC quale sistema gestionale e di comunicazione, ai sensi della normativa vigente, in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili a terzi ad ogni effetto di legge. La casella PEC istituzionale della AOO è cciaa.genova@ge.legalmail.camcom.it e viene utilizzata sia per la trasmissione, che per la ricezione di documenti ed è integrata nel sistema di gestione documentale e protocollo informatico (GEDOC). In ricezione e in trasmissione la casella è configurata sia per la comunicazione con indirizzi PEC, per i quali si riceveranno le ricevute di accettazione/consegna, sia con indirizzi di PEO, per i quali non si riceverà la ricevuta di consegna. Sono attive, inoltre, altre caselle di PEC create esclusivamente per flussi documentali specifici:

- suap@ge.legalmail.camcom.it

- ristori@ge.legalmail.camcom.it
- statisticaprezzi@ge.legalmail.camcom.it
- ufficio.registroimprese@ge.legalmail.camcom.it
- composizione.negoziata@ge.legalmail.camcom.it

4.5 I formati dei documenti informatici

Il formato è la modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

L'obsolescenza dei formati dei file rappresenta una criticità consistente per la conservazione a lungo termine della documentazione la quale, per essere garantita, necessita di una cura continua, che inizia con la corretta scelta del formato già nella fase di gestione documentale.

Per contenere il rischio di obsolescenza occorre utilizzare formati il più possibile "aperti", liberamente utilizzabili e non coperti da brevetto, leggibili da software applicativi gratuiti e *open-source* che possano, a loro volta, essere facilmente reperibili, anche online. I formati dei documenti informatici gestiti dalla Camera sono definiti in conformità all'Allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID con Determinazione n. 407 del 9 settembre 2021 e successivi aggiornamenti. L'elenco dei formati ammessi è aggiornato dal Responsabile della gestione documentale con cadenza almeno annuale, o a seguito di aggiornamenti delle Linee Guida AgID, e pubblicato sul sito istituzionale nella sezione «Amministrazione trasparente».

Di conseguenza, per la creazione e formazione dei documenti nell'AOO si usano i formati DOCX, PDF, PDF/A; i documenti informatici prodotti dalla camera di Commercio, indipendentemente dal software utilizzato, vengono convertiti in formato PDF/A prima della registrazione di protocollo sul Sistema di gestione documentale GEDOC, salvo nei casi in cui essi siano già stati firmati con firma Cades.

Salvo diversamente previsto, agli utenti viene richiesto l'invio di documenti in PDF, PDF/A, JPG, DOCX.

Nell'ambito dei formati dei file trattati non sono ammessi codici integrati quali le cd. "macro" o cifrature dei contenuti, soprattutto per le finalità di conservazione digitale. Non viene consentito l'invio di link esterni da cui scaricare i documenti.

La tabella dei formati riportata nelle pagine seguenti è soggetta a verifica annuale. In caso di obsolescenza di un visualizzatore o di un formato elencato, il Responsabile della gestione documentale provvede all'aggiornamento della tabella con atto unilaterale, acquisita la valutazione tecnica dell'Ufficio CED.

4.6 I metadati dei documenti informatici

Al documento amministrativo informatico sono associati i metadati previsti nel paragrafo 6.3 e ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento nell'allegato n.2. L'immagine seguente (fig. 1) mostra le caratteristiche possedute dai formati che possono maggiormente garantire il principio dell'interoperabilità tra i sistemi di gestione documentale e conservazione.

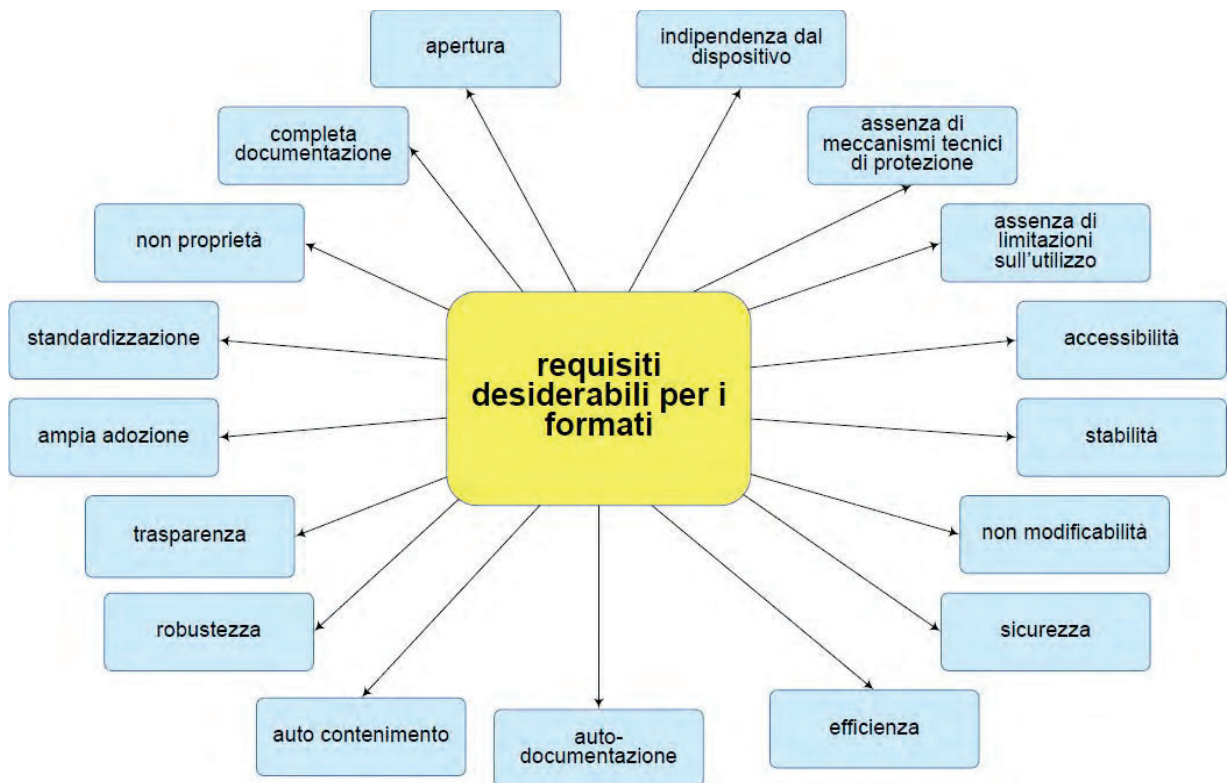


Figura 1 - requisiti dei formati di file

Di seguito, sono elencati i formati di file gestiti dalla Camera (e accettati dal sistema di conservazione di Infocamere):

a) Formati standard raccomandati per la conservazione a lungo termine:

- Documenti impaginati: PDF, ODT, DOCX, ODP, PPTX;
- Fogli di Calcolo : ODS, XLSX;
- Immagini raster: JPG, JPEG, PNG, SVG, TIF, TIFF, ODG;
- Immagini vettoriali: SVG
- Posta elettronica: EML;
- Ipertesti: XML, XBRL;
- Dati strutturati: CSV;
- File di testo: TXT; U3T, U3R
- Applicazioni crittografiche: XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), TSD, M7M;
- Formati fotometrici: IES;
- Contenitori multimediali: MP4;
- Archivi compressi: ZIP;

b) Formati non raccomandati per la conservazione a lungo termine:

- Documenti impaginati: DOC, RTF;
- Fogli di Calcolo: XLS;
- Immagini raster: GIF;
- Immagini vettoriali: DWF;

- Dati strutturati: HTM, HTML;

Nell'ambito di specifici procedimenti vengono utilizzati formati diversi da quelli adottati. Queste eccezioni riguardano essenzialmente documenti ricevuti dall'ente.

I formati compressi (generalmente distinguibili per l'estensione .zip e .rar) possono essere utilizzati solo nel caso in cui i file in essi contenuti sono nei formati accettati dall'amministrazione.

4.7 Sottoscrizione dei documenti informatici

I documenti informatici prodotti o ricevuti dalla Camera che richiedono la sottoscrizione elettronica a valore legale verranno sottoscritti con firma digitale. Le firme digitali adottate dall'ente sono nei formati CADES e PAdES.

I documenti che vanno sottoscritti con firma digitale devono essere prodotti, prima della firma, nel formato standard PDF-A. La data riportata sul documento deve essere coerente con quella dei metadati del documento, della firma digitale e del protocollo informatico. Nel caso di documenti per i quali sia necessaria una data certa e opponibile a terzi, in particolare per i contratti, si renderà necessaria l'apposizione di marca temporale al momento della sottoscrizione.

4.8 La gestione dei documenti cartacei

In ottemperanza alle disposizioni del CAD, l'amministrazione gestisce i documenti analogici solo laddove risulti indispensabile nei rapporti con i soggetti privati che non siano in possesso di un domicilio digitale.

I documenti analogici acquisiti con le modalità tradizionali (consegna allo sportello o ricezione via posta) devono essere digitalizzati, registrati tramite GEDOC ed inseriti all'interno del fascicolo informatico cui si riferiscono ai sensi del piano di fascicolazione.

4.9 Copie e duplicati

Le copie e duplicati di documenti possono essere prodotti secondo le seguenti fattispecie:

- a) **copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico:** consistenti nella scansione di ogni singola unità documentale pervenuta in via analogica. Il documento così acquisito dovrà essere certificato conforme all'originale ai sensi dell'art. 22, comma 2, D.Lgs. n. 82/2005.
- b) **copie analogiche di originali informatici:** stampa dei documenti informatici da inviare ai cittadini sprovvisti di domicilio digitale con l'indicazione del nominativo del soggetto che ha formato il documento, ai sensi dell'art. 3, D.Lgs. n. 39/1993.
- c) **duplicati informatici:** prodotti mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

Copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico:

Per quanto riguarda il punto a) le tipologie di copie informatiche possono essere prodotte nei seguenti modi:

1. **Copia Semplice** (Art. 23, comma 2, D.Lgs. n. 82/2005): viene prodotta tramite la mera scansione e registrazione nel sistema del documento analogico originale. La copia così prodotta ha la stessa efficacia probatoria dell'originale se la sua conformità non è espressamente disconosciuta. Resta fermo l'obbligo di conservazione degli originali analogici, che dovranno essere conservati negli appositi fascicoli cartacei.
2. **Copia Conforme** (Art. 23 comma 1, D.Lgs. n. 82/2005): è accompagnata da una certificazione di conformità e ha la stessa efficacia probatoria dell'originale da cui è tratto.

La certificazione di conformità verrà effettuata dal delegato individuato dal RGD in fase di archiviazione della copia informatica del documento analogico all'interno del fascicolo di pertinenza. Il documento acquisito tramite scanner e la dichiarazione di conformità allegata saranno sottoscritti digitalmente dal delegato. Le copie così formate sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge.

Copie analogiche di originali informatici:

Per quanto riguarda il punto b) le tipologie di copie analogiche possono essere prodotte nei seguenti modi:

1. **Copia Semplice** (Art. 23, comma 2, D.Lgs. n. 82/2005): costituita da una semplice stampa del documento amministrativo informatico. Viene utilizzata in tutti quei casi in cui la natura dell'attività non richieda particolari tutele sul piano giuridico probatorio.
2. **Copia Conforme** (Art. 23 comma 1, D.Lgs. n. 82/2005): ha lo stesso valore del documento informatico da cui è tratta perché, a differenza della prima, viene certificata da un pubblico ufficiale e non può essere disconosciuta dal destinatario (a meno di querela di falso).

La dichiarazione di conformità è prodotta dal sistema GEDOC, e contiene i riferimenti normativi, le indicazioni per identificare univocamente il documento (numero protocollo, data, impronte, numero di pagine), data e luogo di produzione della copia. La dichiarazione deve essere stampata e firmata dal pubblico ufficiale delegato e deve riportare il timbro dell'ufficio (art. 18 DPR. 445/2000).

Le copie analogiche degli atti amministrativi informatici firmati digitalmente, possono essere sottoscritte con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39. La firma autografa sostituita a mezzo stampa consiste nell'indicazione a stampa della fonte e del nominativo del soggetto responsabile, nonché dell'eventuale dicitura che specifica che il documento informatico da cui la copia analogica è tratta è stato prodotto ed è conservato dall'amministrazione secondo come previsto dal Codice.

La firma a stampa può essere utilizzata solo nei rapporti tra l'amministrazione e i privati e solo nei casi in cui il documento non sia una certificazione rilasciata dall'amministrazione.

5 La trasmissione dei documenti

I documenti si distinguono in base allo stato di trasmissione:

- **Documento in ingresso** (mittente esterno e destinatario interno), si intende un documento acquisito dall'AOO nell'esercizio delle proprie funzioni e proveniente da un diverso soggetto pubblico o privato;
- **Documento in uscita** (mittente interno e destinatario esterno), si intende un documento prodotto dalle UO interne dell'AOO nell'esercizio delle proprie funzioni, che ha rilevanza informativa e/o giuridico-probatoria e indirizzato a un diverso soggetto pubblico o privato;
- **Documento interno** si intende un documento prodotto e scambiato internamente (il mittente e il destinatario sono interni). Il documento interno, di norma, non deve essere protocollato.

5.1 Ricezione dei documenti informatici

Un documento informatico può essere ricevuto in diversi modi:

- a mezzo posta elettronica certificata;
- a mezzo cooperazione applicativa;
- a mezzo posta elettronica ordinaria;
- su supporto rimovibile quale, ad esempio, CD ROM, DVD, tape, pen drive, ecc., consegnato direttamente o inviato per posta convenzionale o corriere.

L'amministrazione assicura l'accettazione dei documenti informatici inviati ai suoi uffici tramite i suddetti mezzi quando prodotti in uno dei formati riportati nel presente Manuale.

In tutti gli altri casi, laddove il documento inviato o consegnato all'amministrazione sia prodotto in formati tali da non consentirne una corretta gestione, ne verrà data comunicazione al mittente richiedendo contestualmente la ripetizione dell'invio in uno dei formati indicati nell'elenco o in altro formato concordato. In ogni caso i documenti elettronici inviati o consegnati dovranno essere privi di elementi attivi, tra cui macro e campi variabili.

L'aggiornamento dell'elenco dei formati dei documenti elettronici è curato dal Responsabile della Gestione Documentale.

5.2 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare attraverso:

- servizio postale (posta ordinaria, prioritaria, raccomandata, telegrammi);
- corrieri commerciali e società di recapito convenzionate;
- consegna diretta "brevi manu"

L'accettazione della corrispondenza, recapitata in una delle modalità sopra indicate, avviene, di norma, durante l'intera giornata lavorativa, salvo il caso di consegna allo sportello (per il quale occorre rispettare l'orario di apertura del servizio). La corrispondenza viene recapitata presso l'Ufficio Protocollo, dove viene protocollata e smistata (esclusi i casi di documenti che non necessitano di protocollazione v. par. 6.2).

Il personale addetto al Protocollo tratta la corrispondenza secondo i seguenti tre raggruppamenti:

Tipologia di corrispondenza	Trattamento
Corrispondenza con l'indicazione "personale" o "riservata"	- la busta non è aperta - è trasmessa alla persona indicata o Ufficio competente
Corrispondenza indirizzata a membri di Giunta o Consiglio	- la busta non è aperta - è fatta pervenire all'interessato tramite le Segreteria Generale o la Presidenza
Corrispondenza che non rientra nei due casi precedenti	- la busta è aperta - si procede alla protocollazione (salvo i casi per i quali non è prevista la protocollazione, v. par. 6.2)

Gli addetti al protocollo provvedono alla registrazione, segnatura e scansione dei documenti, con relativo smistamento alle UO di competenza nello stesso giorno di ricezione. Su richiesta dell'interessato viene rilasciata apposita ricevuta della avvenuta registrazione mediante il programma di protocollo informatico o, in alternativa, viene apposta la segnatura di protocollo sulla copia già in possesso dell'utente apponendo la dicitura "copia per l'utente".

5.3 Ricezione della posta elettronica ordinaria

Nel caso in cui sulle caselle di posta elettronica del personale o delle strutture vengano trasmessi messaggi e documenti che devono essere protocollati, questi dovranno essere inoltrati all'apposita casella "Protocollo@ge.camcom.it".

La procedura da seguire prevede che sia scaricato sul proprio pc il messaggio ricevuto e venga allegato all'email da indirizzare all'ufficio protocollo: in questo modo verrà preservata l'integrità del messaggio da protocollare e tutti i riferimenti relativi a mittente, oggetto, destinatario e orario di ricezione della e-mail.

5.4 Ricezione e gestione dei messaggi di posta elettronica certificata

Quando i documenti informatici pervengono all'indirizzo istituzionale di posta elettronica certificata, gli addetti al protocollo procedono alla registrazione.

La casella è gestita dal personale dell'Ufficio protocollo che la consulta giornalmente e valuta, in base alle regole definite nel presente manuale, se il contenuto sia da registrare o meno.

Il sistema GEDOC assicura l'automatica verifica di ricezione di eventuali nuovi messaggi di posta elettronica certificata: è configurato per connettersi alla casella PEC istituzionale mediante protocollo IMAP a intervalli temporali predefiniti, acquisendo automaticamente i messaggi ricevuti e i relativi allegati. All'esito dell'acquisizione, i messaggi vengono rimossi dalla casella di origine e conservati all'interno del sistema di protocollo informatico, che ne garantisce la tracciabilità, l'integrità e la leggibilità nel tempo. In questo modo si ha la certezza che la casella PEC istituzionale non risulti mai piena e sia in grado sempre di ricevere messaggi dall'esterno.

La registrazione di protocollo avviene in conformità a quanto previsto dall'art. 40-bis del D.lgs. 82/2005 (CAD) e dal DPCM 3 dicembre 2013, che disciplinano la gestione dei documenti informatici nelle pubbliche amministrazioni. Ogni messaggio PEC acquisito è trattato come documento informatico ricevuto e sottoposto alle ordinarie operazioni di protocollazione, smistamento e assegnazione. Nel caso in cui venga recapitato per errore una comunicazione non di competenza dell'amministrazione, l'addetto al protocollo trasmette un messaggio al mittente, fornendo - laddove possibile - l'indicazione della pubblica amministrazione a cui indirizzare correttamente la comunicazione.

5.5 Spedizione dei documenti cartacei

La Camera provvede a inviare le comunicazioni ai soggetti che non hanno un domicilio digitale, ovvero nei casi di domicilio digitale non attivo, non funzionante o non raggiungibile, per posta ordinaria o raccomandata con avviso di ricevimento.

Queste comunicazioni sono predisposte come documenti informatici sottoscritti con firma digitale o altra firma elettronica qualificata e archiviati nel Sistema di gestione documentale, secondo le regole riportate nel Piano di fascicolazione. All'utente verrà inviata una copia analogica sottoscritta con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

Nel caso in cui si renda necessario nel corso dell'attività di sportello, gli operatori possono procedere alla consegna a mano di copia analogica dell'originale informatico ai cittadini sprovvisti di domicilio digitale. In ogni caso, all'interno del sistema GEDOC, l'operatore dovrà indicare le modalità di spedizione/consegna del documento all'utente.

5.6 Spedizione dei documenti informatici

I documenti informatici in uscita vengono trasmessi a mezzo posta elettronica certificata, tramite l'applicativo GEDOC.

Il documento informatico principale viene protocollato in uscita dagli uffici di competenza e spedito tramite GEDOC insieme agli allegati utilizzando la casella PEC istituzionale, che è l'unica associata in uscita al registro di protocollo generale dell'ente.

La Posta Elettronica Certificata (PEC) è il vettore privilegiato di relazioni con l'esterno; pertanto, nel caso in cui il destinatario disponga di un domicilio digitale ogni comunicazione formale con esso dovrà essere veicolata tramite questa casella. Se il destinatario non è ancora dotato di un domicilio digitale, allora la spedizione avviene su supporto analogico secondo la procedura descritta nel Manuale.

5.7 Domicilio digitale

Il domicilio digitale permette di facilitare e velocizzare le comunicazioni tra pubbliche amministrazioni.

Per domicilio digitale si intende un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dall'art. 44 del Regolamento (UE) n 910/2014 valido ai fini delle comunicazioni elettroniche aventi valore legale.

L'art. 3 bis del CAD prevede che le pubbliche amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese abbiano l'obbligo di dotarsi di un domicilio digitale iscritto nell'elenco di cui agli articoli 6-bis o 6-ter, ovvero:

- Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IndicePA) [banche dati disponibili e consultabili online].
- Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC)

L'Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi (IndicePA) contiene i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.

Per favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito presso il Ministero per lo sviluppo economico il pubblico elenco, denominato "Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti". La consultazione online degli Indici è consentita a chiunque senza necessità di autenticazione.

I domicili digitali inseriti negli Indici nazionali costituiscono mezzo esclusivo di comunicazione e notifica, secondo quanto previsto dall'art. 6 comma 1 del CAD.

Le comunicazioni tramite i domicili digitali dichiarati negli Indici nazionali producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente. Le comunicazioni si intendono spedite dal mittente se inviate al proprio gestore, e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a un fatto non imputabile al destinatario medesimo. La data e l'ora di trasmissione e ricezione del documento informatico sono opponibili ai terzi.

Ai sensi dell'art. 6-quater del CAD è istituito presso AgID l'Indice Nazionale dei Domicili Digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (INAD). L'INAD, operativo dal 6 luglio 2023, consente alle persone fisiche di eleggere volontariamente un domicilio digitale, ossia un indirizzo PEC o altro recapito qualificato ai sensi del Regolamento eIDAS. La Camera di Commercio, prima di procedere alla spedizione di comunicazioni ai destinatari persone fisiche che non abbiano un domicilio digitale noto, effettua la consultazione dell'INAD, accessibile all'indirizzo www.inad.gov.it, al fine di verificare l'eventuale elezione di un domicilio digitale. Le comunicazioni trasmesse al domicilio digitale risultante dall'INAD producono gli stessi effetti giuridici della notificazione a mezzo posta raccomandata con ricevuta di ritorno.

5.8 Documenti interni

I documenti interni, cioè i documenti prodotti e destinati all'interno dell'AOO della Camera di Commercio di Genova sono formati con tecnologie informatiche. I documenti interni che abbiano un valore formale scambiati tra le UO, vengono inviati attraverso il sistema GEDOC in modo che ne rimanga traccia, e non sussiste l'obbligo della sottoscrizione e della protocollazione. I documenti che rivestono carattere informale possono essere scambiati tra UO attraverso la Posta elettronica o i sistemi informatici interni.

6 La registrazione dei documenti

Per registrazione si intende l'insieme delle procedure, elementi e strumenti attraverso i quali i documenti vengono trattati sotto il profilo strettamente giuridico-probatorio, e dunque il pubblico dipendente che opera nel sistema di protocollazione lo fa in qualità di pubblico ufficiale ed è garante della effettiva ricezione e spedizione dei documenti. La registrazione di protocollo certifica l'acquisizione o la spedizione in data certa di ciascun documento prodotto o ricevuto, indipendentemente dalla loro regolarità, verificata in un secondo tempo dai responsabili dei relativi procedimenti e si configura per la Amministrazione come un'attività obbligatoria.

La registrazione attesta l'esistenza di un determinato documento all'interno del patrimonio documentale dell'Ente, identificandolo univocamente e certifica in modo inoppugnabile, in quanto atto pubblico di fede privilegiata, la data archivistica, dalla quale partono gli effetti giuridici del documento ai sensi della L. 241/1990.

6.1 Documenti soggetti a registrazione di protocollo

Sono oggetto di registrazione obbligatoria ai sensi dell'articolo 53 del DPR n. 445/2000 i documenti ricevuti e inviati dall'amministrazione, che soddisfano i requisiti di competenza soggettiva e oggettiva e hanno un oggetto che riguarda le funzioni di cui l'Ente è competente.

Sono altresì oggetto di registrazione obbligatoria le comunicazioni che provengono da, o sono inviate a, domicili digitali, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida.

La registrazione avviene a cura degli utenti abilitati del sistema GEDOC o, per alcune procedure (come quella relativa al numero meccanografico ITALIANCOM, al Modello Unico di dichiarazione Ambientale MUD, alla trasmissione delle Dichiarazioni di conformità da parte dei Comuni) automaticamente, sulla base di valori definiti dal Responsabile della gestione documentale.

6.2 Documenti non soggetti a registrazione obbligatoria di protocollo

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

- gazzette ufficiali;
- bollettini ufficiali;
- notiziari della pubblica amministrazione;
- materiali statistici;
- bollettini Banco Posta (incasso);
- atti preparatori interni;
- giornali;
- riviste;
- libri;
- opuscoli;
- depliant;
- materiali pubblicitari;
- inviti a manifestazioni che non danno adito ad un'eventuale attivazione di procedimenti amministrativi;

- i documenti già soggetti a registrazione particolare da parte dell'amministrazione;
- documenti di occasione aventi carattere effimero (ringraziamenti, richieste di appuntamenti con i dirigenti, congratulazioni varie, condoglianze, ...);
- tutte le e-mail che si configurano come comunicazioni informali aventi mera natura informativa e non amministrativa, eccetto casi particolari valutati dal Responsabile del procedimento (RdP);

6.3 Registrazione di protocollo dei documenti

La registrazione di protocollo è l'insieme delle informazioni fondamentali relative al contenuto, all'autore e alla modalità di trasmissione di un documento, memorizzate sul registro di protocollo. Questa operazione ha lo scopo di descrivere il documento, individuandolo in modo univoco e di formalizzarne l'ingresso nel sistema documentale rendendone certa l'identificazione e il momento di formazione o entrata. Il numero di protocollo individua un unico documento, compresi i suoi allegati, e dunque ogni documento reca un solo numero di protocollo.

La registrazione di protocollo - sia per i documenti pervenuti in via analogica che telematica - viene effettuata dal personale addetto alla protocollazione mediante il Sistema di gestione documentale GEDOC. Contestualmente alla registrazione viene effettuata dal sistema la segnatura di protocollo.

Di norma la protocollazione avviene lo stesso giorno della ricezione del documento o, al più, il giorno lavorativo successivo se il documento è pervenuto fuori orario. In tal caso si darà priorità alla documentazione pervenuta sulla casella PEC in ordine cronologico di arrivo. Qualora ci sia una ricezione massiva di documenti a fronte di scadenze previste, la protocollazione potrà essere effettuata in differita secondo la procedura descritta nel Manuale.

Tutti gli addetti alla protocollazione sono tenuti al rispetto della riservatezza delle informazioni trattate.

La registrazione di protocollo per ogni documento ricevuto o spedito dalle Amministrazione è effettuata, secondo quanto previsto dall'articolo 53 del DPR 445/2000, mediante la memorizzazione obbligatoria delle seguenti informazioni:

- a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e protocollo del documento ricevuto, se disponibili;
- f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto (assegnata automaticamente dal sistema e registrato in forma non modificabile);

A questi elementi giuridicamente rilevanti se ne possono aggiungere altri, non obbligatori, ma funzionali:

- a) codice fiscale / P.IVA del mittente
- b) numero di protocollo dell'Amministrazione mittente (ove presente) per i documenti ricevuti
- c) data del documento ricevuto
- d) data di arrivo presso l'Ente (solo per il cartaceo)
- e) mezzo di ricezione o di spedizione
- f) attribuzione a UO per competenza o conoscenza
- g) utenti di visibilità del documento
- h) livello di riservatezza
- i) formato del documento (se elettronico o cartaceo)
- j) tipo di documento
- k) classificazione
- l) catalogo dei processi
- m) descrizione sintetica degli allegati
- n) note dell'operatore

6.4 Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento spedito o ricevuto. Essa consente di individuare ciascun documento in modo inequivocabile.

Essa viene generalmente apposta sui documenti in uscita quando questi siano in formato .PDF e siano stati firmati digitalmente con firma PADES. In tutti gli altri casi, la segnatura di protocollo è associata al documento come file .PDF autonomo e la si trova tra gli allegati del documento principale.

L'articolo 55, comma 1, del DPR 445/2000 individua le informazioni che caratterizzano la segnatura di protocollo, ovvero:

- a) codice identificativo dell'amministrazione;
- b) codice identificativo della Camera di Commercio in quanto AOO;
- c) codice identificativo del registro;
- d) progressivo di protocollo;
- e) data di protocollo

Ulteriori informazioni previste sono:

- Indicazione del mittente/destinatario
- la tipologia di Protocollo

Per i documenti protocollati in uscita, se inviati tramite PEC ad altre Amministrazioni viene generato automaticamente un messaggio e-mail conforme alle regole di interoperabilità, che ha in allegato anche il file "segnatura.xml" contenente i dati di segnatura.

6.5 Annullamento e modifica delle registrazioni di protocollo

Le operazioni di annullamento possono riguardare l'intera registrazione (annullamento di informazioni generate automaticamente dal sistema), o le singole informazioni non assegnate automaticamente dal sistema (aggiornamento della registrazione). Il protocollo informatico assicura il tracciamento e la storicizzazione di ogni operazione, rendendole visibili e comparabili.

Modifica delle registrazioni di protocollo

In base alla normativa vigente le uniche informazioni modificabili di una registrazione di protocollo sono l'assegnazione interna all'amministrazione e la classificazione. Tuttavia, è consentita la correzione di meri errori ortografici contenuti nel campo oggetto dei documenti e nel campo mittente per i documenti in entrata. Nel caso in cui le correzioni da effettuare riguardino il contenuto, dovrà essere seguita la procedura prevista per l'annullamento delle registrazioni di protocollo.

Annullamento dell'intera registrazione

Per quanto concerne le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile, l'annullamento anche di una sola di esse determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo. L'operazione di annullamento è autorizzata ed eseguita a cura del Responsabile della gestione documentale o del Vicario su formale richiesta dell'UO che ha effettuato la registrazione. La richiesta deve riportare il numero e la data di protocollo da annullare e i motivi dell'annullamento.

Di seguito, i casi che possono richiedere l'annullamento di una registrazione di protocollo:

- registrazioni di documenti che non sono di competenza dell'Ente;
- registrazioni prodotte erroneamente dal sistema o dai protocollatori;
- registrazioni che recano documenti principali errati/non pertinenti/coerenti con i metadati di registrazione;
- doppie registrazioni di un documento.

Le informazioni relative ad un protocollo annullato rimangono comunque memorizzate per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché gli estremi dell'autorizzazione all'annullamento del protocollo. In tale ipotesi, la dicitura "annullato" è visibile nel dettaglio del documento sul sistema GEDOC, unitamente a tutte le informazioni originarie. Il sistema provvede inoltre a visualizzare la registrazione annullata con caratteri sbarrati, in modo da rendere immediatamente visibile l'avvenuto annullamento.

6.6 Differimento dei termini di registrazione

Nel caso in cui, per eccezionali motivi, non sia possibile procedere alla immediata registrazione di tutta la corrispondenza pervenuta nello stesso giorno di ricevimento e qualora ciò possa pregiudicare un diritto di terzi, il Responsabile della gestione documentale può autorizzare con un motivato provvedimento l'uso del protocollo differito. Il protocollo differito consente la normale registrazione dei documenti con l'evidenziazione della data effettiva di arrivo del documento, oltre che di quella, successiva, di registrazione.

Il provvedimento individua i documenti da ammettere alla protocollazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee, descritte dal Responsabile della gestione documentale nel provvedimento.

6.7 Registro giornaliero di protocollo

Il registro giornaliero di protocollo è un documento informatico prodotto e redatto secondo le modalità previste dalla normativa vigente. Il registro di protocollo è unico e la sua numerazione progressiva è costituita da almeno sette cifre numeriche. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Ai sensi dell'art. 61 comma 2 lettera C del D.lsg 445/2000, il RGD – attraverso procedura automatizzata del sistema GEDOC - entro ciascuna giornata lavorativa, produce il registro giornaliero di protocollo e lo trasmette al sistema di conservazione documentale al fine di assicurarne l'immodificabilità e l'integrità, previa sottoscrizione con firma elettronica qualificata da parte del RGD o di un suo delegato. L'esito dell'invio e la notifica di effettiva conservazione sono comunicati al sistema GEDOC mediante processi automatici.

6.8 Registro annuale di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della data e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici. Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Dopo il 31 gennaio di ogni anno si provvede a trasmettere al sistema di conservazione le registrazioni del protocollo dell'anno precedente. Dal momento che successivamente alla generazione del registro giornaliero potrebbero essere effettuate modifiche sui dati minimi di registrazione, nel registro annuale sarà riportato l'elenco di tutti i protocolli effettuati nell'anno e per ogni protocollo lo storico delle variazioni in termini di annullamento totale o parziale dei campi del protocollo.

Il registro annuale, una volta generato, segue lo stesso flusso di quello giornaliero, con spedizione immediata e automatica al sistema di conservazione dei documenti informatici oppure dopo l'apposizione della firma qualificata. L'esito dell'invio e la notifica di effettiva conservazione sono archiviati in automatico nel sistema.

6.9 Registro di emergenza

Nel caso in cui il protocollo informatico risulti temporaneamente non utilizzabile per un periodo tale per cui la durata della sospensione del servizio possa pregiudicare la registrazione a protocollo in giornata di documentazione soggetta a scadenze inderogabili e prescrittive, i documenti in entrata e in uscita devono essere registrati su un registro alternativo denominato "Registro di emergenza".

Il protocollo di emergenza è avviato, previa autorizzazione del RGD, del Vicario o suo

delegato. Per la registrazione di emergenza può essere utilizzato:

1. Nel caso di disponibilità dei PC un modulo predisposto in formato excel, disponibile nella intranet e compilato mediante l'immissione dei dati direttamente sulla tabella.
2. Nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modulo allegato al Manuale di gestione che verrà compilato manualmente (v. Allegato n.3)

Una volta ripristinate le normali funzionalità del sistema, il servizio di Protocollo, provvede a registrare sul registro generale di protocollo i relativi protocolli di "emergenza". Sul registro di emergenza deve essere riportata la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino delle funzionalità del sistema, ed eventuali annotazioni ritenute rilevanti dal Responsabile della gestione documentale.

Prima di autorizzare l'avvio della procedura, il Responsabile del Servizio archivistico deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza. Ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Il Responsabile del Servizio archivistico dovrà annotare nel protocollo informatico unico i periodi di attivazione del Registro di emergenza e, nel caso in cui nel corso dell'anno non si sia fatto ricorso al Registro di emergenza, anche il mancato uso.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, UO, anno di registrazione, numero di protocollo nel formato stabilito. La segnatura del protocollo di emergenza deve essere apposta mediante timbro o altro dispositivo e riportare le informazioni desunte dal relativo registro.

Una volta ripristinata la piena funzionalità del sistema, il Responsabile della gestione documentale effettua la chiusura dei registri di emergenza, e annota su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura. Il periodo massimo di autorizzazione all'utilizzo del registro di emergenza è pari ad una settimana ed in ogni caso devono essere riportati gli estremi del provvedimento di autorizzazione nel registro stesso.

La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico e ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo a partire dal numero successivo all'ultimo registrato prima dell'interruzione.

A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza. Di conseguenza, i documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico saranno contraddistinti da due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

7 Casi particolari

7.1 Documentazione soggetta a registrazione particolare

In quanto soggetti a normativa separata, oltre al protocollo generale della Camera di Commercio sono soggetti a modalità di registrazione particolare:

1. le denunce al Registro Imprese;
2. le richieste di certificati d'Origine e Carnet ATA;
3. Il protocollo dello Sportello Unico per le Attività Produttive (SUAP)
4. i Protesti cambiari
5. le domande della Carta del Conducente.
6. le domande di brevetti e marchi
7. Le serie delle delibere e comunicazioni della Giunta e del Consiglio e delle determinazioni del Segretario Generale

REGISTRO DELLE DENUNCE AL REGISTRO DELLE IMPRESE E ALL'ALBO IMPRESE ARTIGIANE

Sono soggette a registrazione particolare:

- le domande di iscrizione, modifica o cancellazione dal R.I.

Tutte le altre tipologie di documento non sono soggette a registrazione particolare da parte dell'Ufficio R.I. e sono registrate nel protocollo generale dell'Ente:

- le richieste di accertamento inviate a coloro che hanno presentato le domande
- l'invio dei suddetti accertamenti da parte dei diretti interessati
- le richieste di visure /certificati/elenchi inviate per posta
- l'invio di visure /certificati/elenchi
- dichiarazioni di fallimento e tutto ciò che attiene alle procedure concorsuali (concordati preventivi e fallimentari, stato di insolvenza, liquidazioni coatte)

PRATICHE SUAP

- Segnalazione Certificata di Inizio Attività
- Comunicazioni agli enti terzi
- Comunicazione REA
- Comunicazione esito REA

DELIBERE, COMUNICAZIONI E DETERMINAZIONI

Le delibere e comunicazioni di Giunta, le delibere del Consiglio e le determinazioni in quanto documenti già soggetti a registrazione particolare da parte dell'Amministrazione non vanno registrati nel protocollo generale. A ciascuna delibera o determinazione è associato un numero di repertorio di efficacia giuridico-probatoria. Ciascun complesso delle delibere, delle comunicazioni e delle determinazioni costituisce una serie. Ciascuna serie deve essere corredata da un proprio repertorio generale.

Nel repertorio generale va riportato un numero progressivo, denominato “numero di repertorio”, che identifica il documento all’interno della serie. Il repertorio generale ha cadenza annuale, cioè inizia il 1° gennaio e termina il 31 dicembre di ogni anno. Sono istituiti i seguenti repertori:

- Le delibere della Giunta Camerale e le comunicazioni del Presidente alla Giunta camerale;
- Le delibere del Consiglio Camerale;
- Le determinazioni d’urgenza del Presidente;
- Le determinazioni del Segretario Generale e dei Dirigenti.

REGISTRO DEI VERBALI DI SEDUTA

Le seguenti tipologie di documento sono soggette a registrazione particolare annuale progressiva da parte dell'Ufficio Affari Generali:

- verbali della Giunta Camerale
- verbali del Consiglio Camerale

Ciascun verbale di seduta contiene le deliberazioni adottate in quella data ed è corredato da un proprio repertorio generale.

REGISTRO DEI PROTESTI CAMBIARI

Sono soggette a registrazione particolare da parte dell’Ufficio:

- l’elenco Protesti consegnato dall’Ufficiale Levatore
- i decreti di riabilitazione
- le richieste di annotazione sugli effetti cambiari
- le istanze di cancellazione dal registro protesti

Non sono soggette a registrazione particolare da parte dell’Ufficio e sono registrate nel protocollo generale dell’Ente, tutte le altre tipologie di documento, quali, ad es.:

- 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

7.2 Documenti a carattere riservato, personale e/o confidenziale

La corrispondenza che rechi nell'oggetto la dicitura "personale", "riservato", "s.p.m." e destinata al personale dipendente deve essere direttamente assegnata al destinatario il quale, dopo averne preso visione, deciderà se farla protocollare o meno. In caso affermativo, l'addetto al protocollo che effettua la registrazione di protocollo in ingresso o in uscita attribuisce al documento il livello di riservatezza/visibilità necessario in base a criteri definiti da procedure interne o su indicazione del responsabile del documento.

7.3 Lettere anonime

Tutte le lettere anonime non sono soggette a protocollazione, ma devono essere sottoposte all'attenzione del Segretario generale o di persona da lui stesso delegata ed eventualmente al Responsabile della UO competente per materia. È comunque garantita la protocollazione delle comunicazioni anonime inviate al Responsabile per la prevenzione della corruzione, nominato ai sensi dell'art. 1 Legge n. 190/2012.

7.4 Documenti non firmati o con firma illeggibile

I documenti non firmati per i quali è possibile individuare il mittente vengono protocollati indicando, nel sistema GEDOC, la circostanza che si tratta di "Documento privo di sottoscrizione". Nel caso in cui il documento in questione sia parte della documentazione relativa ad un determinato procedimento, l'eventuale regolarizzazione sarà disposta a discrezione del responsabile del procedimento (RdP).

7.5 Documentazione di competenza di altre amministrazioni o uffici

Nel caso in cui pervenga erroneamente ad un Ufficio documentazione sulla quale lo stesso non abbia competenza, il responsabile può provvedere a riassegnarlo all'Ufficio competente oppure ne dà notizia all'ufficio protocollo che provvederà a riassegnare i documenti. Nel caso in cui la Camera di Commercio riceva documentazione indirizzata ad altra Amministrazione, l'ufficio Protocollo - in virtù del principio di leale collaborazione tra amministrazione e privati - provvederà a inviare al mittente un messaggio contenente l'indicazione del recapito corretto, se individuabile. Nel caso in cui questa documentazione venga protocollata per errore si dovrà procedere all'annullamento della registrazione (vedi paragrafo 6.5).

7.6 Documento inviato a più UO e/o pervenuto attraverso canali diversi

Uno stesso documento potrebbe pervenire tramite canali diversi (consegna a mano, invio postale, invio telematico) o, ancora, potrebbe essere indirizzato a più destinatari. In questi casi, l'addetto prima di protocollarlo deve verificare attraverso il sistema informatico che esso non sia già stato registrato per evitare doppie registrazioni.

Anche se pervenuto in più esemplari, un documento deve essere individuato da un solo ed unico numero di protocollo, ma qualora questo documento sia già stato registrato più volte, ai fini del calcolo dei tempi del procedimento

amministrativo si dovrà tener conto della data archivistica di quello protocollato per primo.

7.7 Oggetti plurimi

Ogni documento protocollato in entrata o in uscita dovrebbe obbligatoriamente trattare un solo oggetto e riferirsi ad un unico procedimento. Nel caso in cui, un documento tratti una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e a fascicoli diversi, l'addetto alla registrazione deve smistare il documento acquisito a sistema alle UO competenti che provvederanno a:

- multifascicolarlo, in modo che esso risulti agli atti in ogni fascicolo di pertinenza
- multiclassificarlo, ove necessario, in base alla natura dei singoli procedimenti interessati

8 Assegnazione e classificazione dei documenti

8.1 Assegnazione

L'assegnazione è l'operazione che consente di tracciare ogni passaggio del documento e dei fascicoli per competenza o per conoscenza, al fine di garantire la massima trasparenza nell'ambito di qualsiasi procedimento amministrativo.

Il dirigente di ciascuna UO provvede ad assegnare a sé, o altro dipendente addetto all'unità, la responsabilità dell'istruttoria e di ogni altro adempimento inerente al singolo procedimento nonché, eventualmente, dell'adozione del provvedimento finale. Fino a quando non sia effettuata l'assegnazione è considerato responsabile del singolo procedimento il funzionario preposto alla UO competente.

Tutte le assegnazioni sono tracciate dal sistema: GEDOC memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

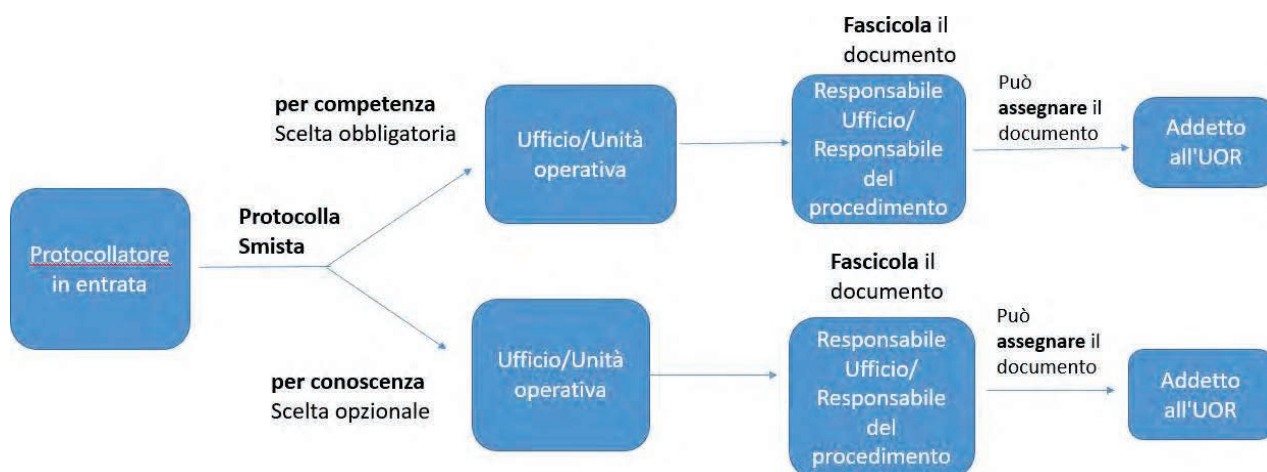


Figura 1 Flusso di smistamento e assegnazione dei documenti

I passaggi illustrati in figura sono descritti di seguito:

1. A seguito della protocollazione, un documento viene smistato all'ufficio/unità operativa (UO) competente.
2. Con l'assegnazione del documento a un ufficio si provvede al conferimento della responsabilità del procedimento amministrativo al responsabile Ufficio, che potrà prendere in carico il documento o, a sua volta, assegnarlo ad un collaboratore attraverso l'apposita funzione prevista da GEDOC.

Il sistema GEDOC prevede le seguenti assegnazioni:

- **Assegnatario competenza (obbligatorio):** identificazione dell'UO a cui è attribuita la responsabilità dei procedimenti attivati dal documento o ai quali il documento è correlato. Attraverso questa funzione, il documento verrà visualizzato nella scrivania del responsabile del procedimento (RdP)/responsabile Ufficio tra i documenti da assegnare.

- **Assegnatari per conoscenza:** indica le UO che, a vario titolo, possono essere interessate a conoscere un documento. Il responsabile del procedimento (RdP)/responsabile d'ufficio del potrà visualizzarlo tra i documenti assegnati per conoscenza e eventualmente prenderlo in carico per lavorarlo a sua volta.
- **Utenti a cui è assegnata la visibilità:** sono soggetti appartenenti a uno o più uffici che devono poter avere accesso a un documento. In questo caso non si tratta di una vera e propria assegnazione; pertanto, il sistema non ne darà immediata evidenza, ma il documento potrà essere consultato attraverso le apposite funzioni di ricerca.

È possibile selezionare l'assegnatario dallo schema dell'organigramma reso navigabile da GEDOC. In fase di smistamento i documenti devono essere assegnati preferibilmente ad un'unica UO di competenza per non appesantire le successive operazioni di archiviazione e di eliminazione dei documenti dalle scrivanie degli uffici. Gli uffici scelti per conoscenza possono, invece, essere molteplici.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.

8.2 Modifica delle assegnazioni

In caso di errato smistamento l'UO assegnataria può:

- Rimandare il documento al Protocollo informandolo dell'errore attraverso il campo note disponibile in GEDOC.
- Smistare in autonomia la notifica ad altra UO.

Gli operatori di protocollo possono riassegnare il documento ad altra struttura di competenza.

È possibile aggiungere altri uffici in conoscenza ad un documento assegnato: possono farlo gli utenti dell'ufficio che hanno inserito il documento, ovvero ogni altro per ufficio per cui il documento è in competenza. L'aggiunta di uffici assegnatari "in conoscenza" è ammessa per soli documenti "non riservati". Dalle funzioni di assegnazione del documento si possono selezionare gli uffici tra l'elenco dei possibili assegnatari per conoscenza, selezionandoli dall'organigramma dell'Ente.

8.3 Consegna dei documenti cartacei

Nel caso di ricezione di documenti cartacei (consegnati a mano o per mezzo di vettore postale), gli addetti al protocollo verificano innanzitutto la completezza della documentazione (es. corretto destinatario, presenza sottoscrizione autografa) e procedono alla scansione e alla verifica della rispondenza del documento digitalizzato (copia informatica del documento analogico) all'originale cartaceo.

Successivamente gli addetti procedono alla protocollazione, alla segnatura e all'assegnazione dei documenti, indicando nel campo Annotazioni della scheda documentale eventuali rilievi/osservazioni sulle verifiche effettuate.

La procedura di scansione e le successive verifiche di rispondenza precedono l'attestazione di conformità della copia dei documenti informatici all'originale che deve essere effettuata per il tramite dell'apposita procedura presente in GEDOC e sottoscritta mediante la firma digitale dell'operatore.

8.4 Consegna dei documenti informatici

La ricezione dei documenti informatici indirizzati all'Amministrazione è assicurata tramite la casella di posta elettronica istituzionale. Nel caso in cui un documento venga ricevuto sulla PEO dell'Ufficio, il destinatario deve invitare il mittente a inviare il documento alla casella di posta elettronica istituzionale agganciata in Gedoc.

Nel caso in cui l'Ufficio decidesse di accettare la PEO occorre seguire la procedura descritta nel paragrafo 5.3.

8.5 Classificazione dei documenti

La classificazione è un'attività obbligatoria che permette la corretta organizzazione dei documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'amministrazione e consente di ordinare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

Tutti i documenti, in entrata e in uscita, indipendentemente dal supporto sul quale vengono formati e dalla loro protocollazione o meno, devono essere classificati in base al Piano di classificazione adottato dall'ente.

Il Piano di classificazione è strutturato tenendo conto delle funzioni svolte dall'Amministrazione e non si basa sulla struttura organizzativa. Si configura come uno schema generale di 'voci' articolate in modo gerarchico, partendo da quelle a carattere generale (Titoli) fino ad arrivare a quelle di carattere particolare (Classi e sottoclassi), al fine di identificare secondo uno schema logico i documenti e i fascicoli.

Classificare vuol dire attribuire, in fase di inserimento di un documento informatico in GEDOC, o in seguito alla sua assegnazione nel caso si tratti di un documento in entrata, un indice di classificazione desunto dal Piano di classificazione. La classificazione è propedeutica all'attività di fascicolazione e uno stesso documento può essere classificato più volte, in base alla molteplicità di funzioni individuate, e associato a più fascicoli.

Eventuali modifiche alla classificazione di un documento sono possibili da parte degli utenti abilitati alla funzione e sono tracciate nel sistema.

La revisione, anche parziale, del Piano di classificazione viene proposta dal RSP quando necessario ed opportuno. Dopo ogni modifica il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

La Camera di Commercio utilizza il Piano di classificazione adottato con Delibera di Giunta n.248 del 13 settembre 2021.

Il Piano di classificazione non è retroattivo: non si applica, cioè, ai documenti archiviati prima della sua introduzione.

9 Fascicolazione dei documenti

9.1 Formazione dei fascicoli

L'archivio è il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività.

Ai sensi dell'art. 52 del DPR 28 dicembre 2000, n. 445 il sistema di gestione informatica dei documenti, in forma abbreviata «sistema» deve:

- a) garantire la sicurezza e l'integrità del sistema;
- b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
- c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
- e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Tutti i documenti registrati nel sistema informatico e classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli, ad eccezione di tutto quanto attiene i materiali preparatori e di lavoro per arrivare alla formazione del documento (bozze, proposte, primi elaborati, report di controllo, appunti ecc.). Nel sistema di gestione documentale si collocano solo i documenti nella loro versione definitiva, salvo casi in cui ci siano particolari esigenze di tenere traccia di alcuni passaggi nella formazione del documento o di dividerne il contenuto già in questa forma con altri.

La fascicolazione è l'attività attraverso cui un documento viene ricondotto logicamente all'interno dell'unità archivistica assieme ai documenti precedenti, e che mantiene vivo il **vincolo archivistico** che lega ogni singolo documento alla pratica di cui fa parte (ordine cronologico di sedimentazione). Questa attività permette di costruire un sistema basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore dell'archivio. La fascicolazione è obbligatoria per tutti i documenti, anche quelli non protocollati.

Il **fascicolo** è lo strumento operativo per organizzare i documenti all'interno di un archivio ed è l'unità primaria e fondamentale di conservazione dei documenti. Esso costituisce la raccolta ordinata della documentazione prodotta e accumulata nel corso della trattazione di un affare/procedimento o riguardante un determinato oggetto.

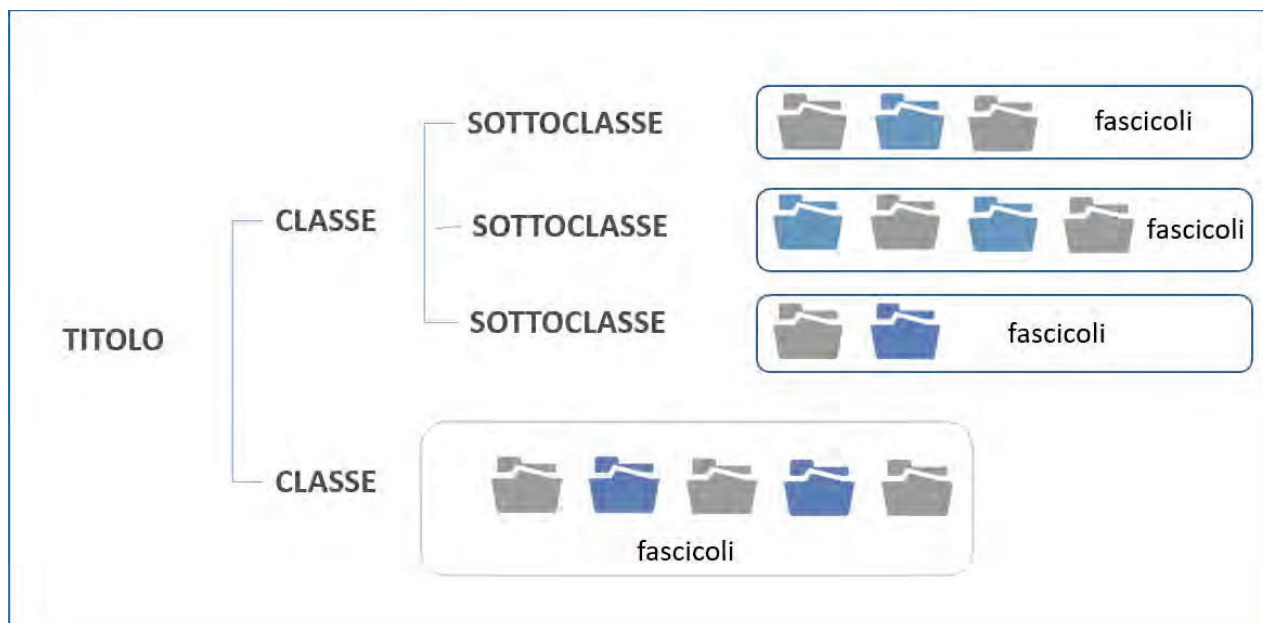


Figura 2 Piano di fascicolazione – schema

I fascicoli si aprono al livello più basso del Piano di classificazione (classe o sottoclasse) e non costituiscono un ulteriore livello, come mostrato in figura.

9.2 Tipologie di fascicolo

I fascicoli possono essere suddivisi in tipologie che variano a seconda della natura dei documenti da inserire e della loro organizzazione interna.

Le tipologie di fascicoli sono cinque:

1. Fascicolo procedimentale

Il fascicolo procedimentale è un fascicolo che raccoglie tutta la documentazione relativa a un procedimento amministrativo e, in base alla complessità e alla numerosità della documentazione prodotta, può essere articolato in sottofascicoli che rispecchiano le fasi del procedimento. Nella generalità dei casi esse sono:

1. fase dell'iniziativa;
2. fase istruttoria;
3. fase costitutiva;
4. fase integrativa dell'efficacia.

La durata di un fascicolo per procedimento equivale alla durata del procedimento stesso.

2. Fascicolo per affare

Il fascicolo per affare raggruppa in un unico fascicolo i documenti relativi ad una competenza che non prevede l'adozione di un provvedimento finale. Può essere articolato in sottofascicoli in base alla complessità e alla numerosità della documentazione prodotta e la sua durata può essere pluriennale.

3. Fascicolo per attività

Il fascicolo per attività è costituito dai documenti prodotti nel corso dello svolgimento di attività semplici, che non afferiscono a un procedimento amministrativo e non richiedono l'istruzione di un fascicolo per affare, esaurendosi in risposte obbligate o in meri adempimenti di legge.

Il fascicolo per attività si apre e si chiude nell'ambito dell'anno di gestione.

4. Fascicolo di persona fisica

E' anche conosciuto come fascicolo per oggetto o nominativo o persona e si utilizza per raggruppare tutti i documenti relativi ad una persona fisica, anche relativi a procedimento diversi.

Tipico è il caso dei fascicoli del personale, dove tutta la documentazione di un dipendente è racchiusa in un fascicolo, suddiviso a sua volta in sottofascicoli.

La durata del fascicolo per persona fisica è in genere pluriennale, in quanto legata alla durata della relativa materia/oggetto.

5. Fascicolo di persona giuridica

Il fascicolo di persona giuridica, come il precedente, conserva documenti relativi a diversi procedimenti amministrativi, distinti affari o diverse attività, ma legati da un vincolo archivistico interno, relativo ad una persona giuridica.

Anche i fascicoli intestati alle persone giuridiche possono avere durata pluriennale.

9.3 Struttura gerarchica del fascicolo

Un **fascicolo** può essere articolato in **sottofascicoli**, e questi in **inserti**, con l'obiettivo di facilitare la gestione, l'accessibilità, il reperimento e la selezione della documentazione in esso contenuta.

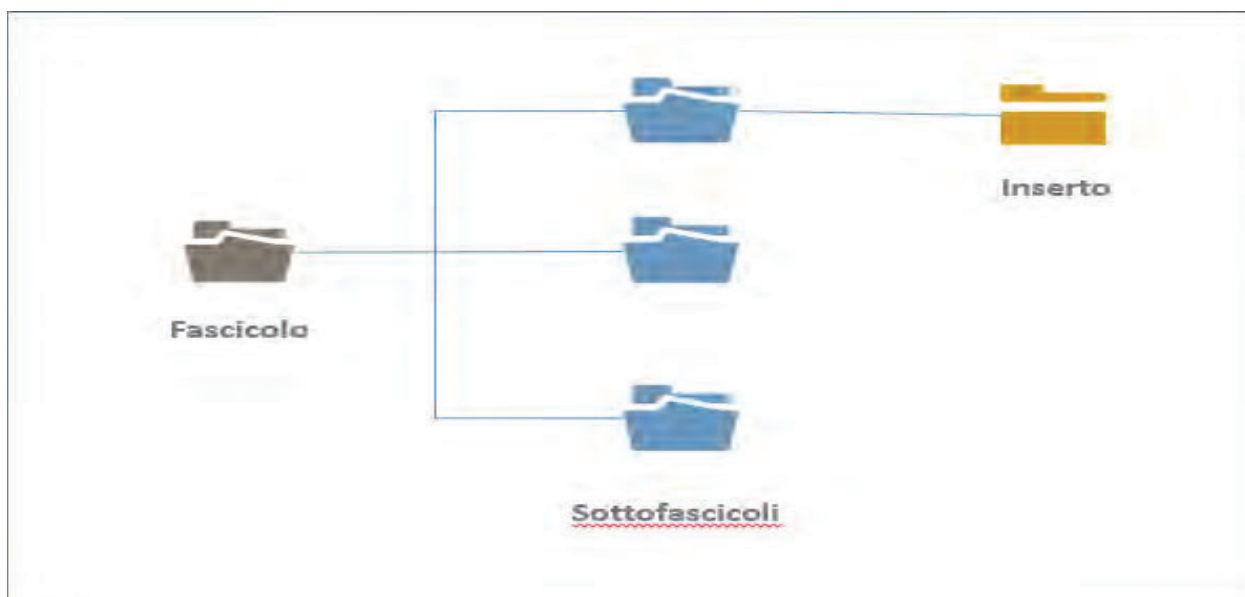


Figura 3 Articolazione interna del fascicolo

Le buone prassi archivistiche sconsigliano di andare oltre nella suddivisione del fascicolo, cosa che avrebbe l'effetto di appesantire il governo della documentazione.

Alcune tipologie di fascicoli rendono necessaria la suddivisione dei documenti in modo articolato a causa della quantità, dell'articolazione del loro contenuto, delle varie fasi del procedimento cui afferiscono, del livello di riservatezza attribuito alla documentazione e delle differenze nei tempi di conservazione: un fascicolo può contenere, infatti, documentazione con una valenza temporale limitata e documenti soggetti a conservazione illimitata.

Sono riportati, di seguito, alcuni esempi che non devono, tuttavia, essere interpretati in modo rigido:

Fascicoli relativi ad eventi, iniziative, progetti:

Si tratta di fascicoli per affare che possono avere durata pluriennale e possono essere articolati in sottofascicoli relativi a ciascuna fase dell'iniziativa, anche se si tratta di fasi non standardizzate come quelle di un procedimento.

Fascicoli relativi a organismi

Si tratta di un fascicolo che gestisce l'organizzazione/gestione di un organismo (ad esempio Gruppi di lavoro, commissioni ecc.). Per gli organismi complessi si può considerare un'articolazione in sottofascicoli, ad esempio:

- Parte istituzionale: costituzione, funzionamento, normativa e organi (deleghe)
- Attività e funzionamento: riunioni degli organi, atti e verbali
- Gestione iter elaborazione, progettazione e organizzazione: corrispondenza, documenti istruttori, bozze preparatorie
- Progetti e azioni specifiche: progetti, proposte, interventi

Un caso particolare riguarda la documentazione prodotta dai cosiddetti "tavoli o gruppi di studio", che consta solitamente di report relativi all'analisi di determinati fenomeni. Nel caso in cui queste attività abbiano una cadenza periodica, è possibile creare un fascicolo per ciascun gruppo. Nel caso in cui la cadenza fosse episodica, la documentazione potrebbe essere organizzata in fascicoli per iniziativa.

Bandi per contributi

Si tratta di fascicoli procedurali che possono articolarsi in sottofascicoli relativi a:

- Gestione generale del bando
- Richieste di contributo, istruttoria e valutazione ammissibilità
- Comunicazione esito richiesta
- Comunicazione liquidazione contributo
- Rendicontazione contributo e esiti attività
- Visite ispettive e controlli

Fascicoli personali

I fascicoli del personale sono destinati alla conservazione permanente e si riferiscono al personale in servizio e in quiescenza, di ruolo e non di ruolo. Essi sono relativi a ciascun dipendente e hanno una strutturazione interna articolata e complessa. I sottofascicoli possono essere creati in base alle varie fasi del rapporto di lavoro, a quelle della gestione dell'aspetto economico o dell'aspetto normativo.

9.4 Processo di identificazione e formazione dei fascicoli

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, di un'attività istruttoria, di un'attività continuativa, anche relativa a un soggetto giuridico o a una persona fisica (es. personale), il funzionario preposto provvede all'apertura di un nuovo fascicolo.

I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, di un sottofascicolo/inserto, secondo l'ordine cronologico di registrazione.

Con la formazione di un nuovo fascicolo si provvederà a registrare nel sistema informatico le seguenti informazioni:

- indice di classificazione;
- numero del fascicolo (assegnato automaticamente dal sistema);
- oggetto del fascicolo;
- data di apertura (assegnata automaticamente dal sistema);
- responsabile del procedimento;

Quando i documenti vengono associati al fascicolo ne assumono la voce di classificazione, se non già attribuita a livello di documento.

L'oggetto (o descrizione) del fascicolo deve essere strutturato secondo criteri uniformi e condivisi per evitare:

- inefficienza nella ricerca;
- difformità nella redazione dell'oggetto di fascicoli omologhi;
- difficoltà a identificare il contenuto di un fascicolo;

Il Piano di fascicolazione adottato dalla Camera di Commercio propone un'organizzazione delle informazioni costruita intorno alle seguenti regole:

- le informazioni devono seguire una gerarchia dal generale al particolare;
- è bene evitare singole parole generiche (indagini, ricerche, attestazioni, certificazioni, comunicazioni ecc.);
- si devono utilizzare brevi frasi di senso compiuto che forniscano indicazioni chiare sul contenuto del fascicolo (ovvero l'affare / attività / procedimento amministrativo ecc.) ;
- si devono inserire nella descrizione le "parole chiave", laddove possibile;
- nel caso di fascicoli che si ripetono nel tempo, indicare l'anno di riferimento (o altre informazioni distintive) per differenziarli;
- la descrizione di un fascicolo deve essere sempre diversa da quella di un altro.

9.5 Alimentazione dei fascicoli

I fascicoli correnti sono conservati nel sistema di gestione documentale e possono essere alimentati dal responsabile del fascicolo, da eventuali suoi incaricati, oppure da una o più UO nell'ambito dello stesso procedimento amministrativo.

Il fascicolo deve essere chiuso al termine del procedimento amministrativo, dell'istruttoria o dell'attività cui si riferisce, oppure su base temporale (per esempio alla fine dell'anno solare se si tratta di un fascicolo di attività).

9.6 Conservazione dei fascicoli

I documenti e i fascicoli sono archiviati sul sistema informatico GEDOC ed inviati automaticamente al sistema di conservazione, sulla base delle regole stabilite nel Manuale di conservazione della Camera di Commercio.

I fascicoli vengono inviati in conservazione dopo 30 giorni dalla chiusura.

Il sistema di gestione documentale mantiene in forma di duplicato i fascicoli e i documenti già inviati in conservazione finché essi sono necessari allo svolgimento delle attività: pertanto è possibile continuare a consultare il contenuto di un fascicolo anche dopo il suo invio in conservazione.

9.7 Gestione dello scarto

Lo scarto di documenti degli archivi della pubblica amministrazione è soggetto alla preventiva autorizzazione della Soprintendenza archivistica, secondo quanto disposto dall'art. 21, comma 1, lettera d) del Codice dei Beni Culturali.

Il Piano di conservazione stabilisce le tempistiche di conservazione e di scarto tenendo conto sia della normativa di riferimento sia dell'analisi interna effettuata dal RGD, congiuntamente con le UO responsabili del trattamento dei documenti.

I termini minimi di conservazione vanno intesi dalla data di chiusura del fascicolo in via generale, salvo contenzioso in essere, e sono periodicamente verificati alla luce di nuove possibili normative di settore che obbligano ad un periodo di conservazione maggiore rispetto a quello indicato alla data di emanazione del Piano di conservazione dei documenti.

Le modalità di scarto dei documenti e dei fascicoli elettronici contenuti nei pacchetti di archiviazione sono concordate tra la Camera di Commercio e il Conservatore (InfoCamere) e descritte nel Manuale di conservazione del Conservatore.

Periodicamente, il Responsabile della gestione documentale predispone, con propria determinazione, l'elenco del materiale documentario da scartare, al fine di ottenere la necessaria autorizzazione della Soprintendenza archivistica competente.

Il Responsabile della gestione documentale invia alla Soprintendenza archivistica una lettera formale con la richiesta di autorizzazione allo scarto di atti d'archivio, accompagnata da un elenco dettagliato della documentazione che intende eliminare, in duplice copia.

L'elenco deve contenere almeno i seguenti dati:

- tipologia dei documenti da scartare e relativo indice di classificazione; per una chiara individuazione delle tipologie documentarie è consigliabile utilizzare, laddove possibile, la terminologia impiegata nel Piano di conservazione di riferimento; inoltre, per ciascuna tipologia individuata:
- estremi cronologici della documentazione;
- numero dei pezzi, da quantificare in buste, registri, scatole, metri lineari etc.;
- peso (in Kg per la documentazione analogica, KB, MB ecc. per quella digitale)
- motivazione della proposta di scarto.

Dopo un attento esame, che comprende il raffronto con le indicazioni del Piano di conservazione, la Soprintendenza può autorizzare la distruzione integrale o parziale dei documenti indicati nell'elenco, ovvero respingere la richiesta sulla base di motivazioni che verrebbero di volta in volta esposte.

La Soprintendenza ha l'obbligo di concludere il procedimento entro il termine di 60 giorni dalla ricezione della proposta, fatte salve eventuali richieste di ulteriori informazioni circa i materiali che si intendono scartare, che sospenderebbero la decorrenza del termine.

Qualora l'autorizzazione venga rilasciata, la documentazione analogica da eliminare dovrà essere consegnata a una ditta specializzata o ad altre organizzazioni che ne garantiscano in modo certo la distruzione. Particolare attenzione dovrà essere posta ai documenti contenenti dati sensibili, che dovranno essere salvaguardati ai sensi della vigente normativa sulla privacy e dei quali si dovrà evitare ogni possibile uso improprio.

Nel caso di documentazione digitale, la richiesta di scarto e il conseguente provvedimento autorizzatorio dovranno essere trasmessi al Conservatore affinché provveda alla distruzione della documentazione contenuta nei pacchetti di archiviazione. L'operazione di scarto viene tracciata sul sistema di conservazione mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e la sua autorizzazione.

Il verbale di avvenuta distruzione dei documenti, rilasciato dal soggetto incaricato della distruzione della documentazione (sia essa analogica o digitale), dovrà essere trasmesso alla Soprintendenza archivistica entro 60 giorni, per la conclusione del procedimento.

I documenti e i fascicoli sottoposti a scarto nel sistema di conservazione saranno eliminati anche dal sistema di gestione documentale e dagli altri applicativi integrati.

10 Scansione dei documenti cartacei

Tutti i documenti di rilievo per l'Ente devono essere inseriti e gestiti nel sistema di gestione documentale che rappresenta l'archivio unico informatico della Camera di Commercio. Pertanto, la documentazione cartacea pervenuta in Camera di Commercio deve essere convertita in digitale mediante processi e strumenti che assicurino che i documenti informatici abbiano contenuto e forma identici a quelli dei documenti analogici da cui sono tratti, come previsto dall'art 22 del CAD. Per assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto sono previste dalla normativa due modalità:

1. Raffronto dei documenti e relativa certificazione di conformità
2. Certificazione di processo mediante tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia

10.1 Processo di scansione e certificazione di conformità

Il procedimento di scansione dei documenti analogici e di apposizione della certificazione di conformità si articola nelle seguenti fasi:

- scansione del documento analogico ed ottenimento di un file PDF. Ad un documento, anche composto da più pagine, deve corrispondere un unico file.
- verifica della correttezza dell'acquisizione delle immagini mediante raffronto con l'originale,
- redazione dell'attestazione di conformità del documento informatico al documento analogico da cui è tratto, generata nell'ambito del sistema GEDOC;
- apposizione della firma digitale al documento così ottenuto da parte del personale a ciò autorizzato.

Gli utenti abilitati, provvedono alla scansione dei documenti secondo le opzioni previste dalla procedura, ovvero all'acquisizione diretta tramite scanner del file in formato PDF salvandolo in una directory interna e riservata alla Camera, accessibile dall'operatore che procederà all'acquisizione in Gedoc del documento. È a carico dell'operatore la verifica visiva della corrispondenza in termini di contenuti tra il documento originale analogico e il documento scansionato. Il documento informatico così prodotto viene inserito come documento in ingresso nel sistema di gestione documentale, che chiederà all'utente di specificare il formato del documento originale. In questo caso, l'utente dovrà selezionare "cartaceo".

Effettuata l'acquisizione del documento, il sistema di gestione documentale verifica il formato del file acquisito (PDF/A), conta il numero di pagine e produce un documento in formato PDF/A di contenuto identico, ma con l'aggiunta in ultima pagina dell'attestazione di conformità con l'evidenza del pubblico ufficiale che la firmerà digitalmente.

Il documento da firmare digitalmente è, quindi, comprensivo sia dei contenuti del documento analogico originale, che dell'attestazione di conformità. La firma digitale dell'attestazione di conformità è permessa a utenti ai quali è stato attribuito uno specifico ruolo funzionale del sistema di gestione documentale, nello specifico sono esclusivamente gli addetti all'Ufficio Protocollo, unico ufficio che può effettuare la protocollazione in entrata. Il documento informatico così prodotto viene inserito come documento in ingresso nel sistema di gestione documentale con l'attribuzione dei metadati minimi obbligatori, tra cui l'impronta del documento che viene generata in automatico dal sistema.

11 Gestione documenti cartacei degli archivi di deposito

L'archivio di deposito è costituito dai documenti relativi ad affari e a procedimenti amministrativi di cui è terminata la trattazione e che richiedono un accesso poco frequente. Nell'archivio di deposito vengono effettuate le operazioni di selezione e scarto della documentazione in base ai criteri indicati Piano di conservazione:

- i documenti digitali relativi ad affari conclusi sono archiviati in GEDOC e nel Sistema di conservazione.
- i documenti originali cartacei, acquisiti o meno nel sistema di gestione documentale come copie digitali, devono essere archiviati e conservati secondo le modalità descritte di seguito e per i tempi previsti dal Piano di conservazione.

11.1 Gli archivi di deposito delle Unità organizzative (UO)

Ciascuna UO conserva i fascicoli cartacei relativi ad affari e procedimenti amministrativi conclusi o comunque non più necessari ad una trattazione corrente all'interno dei propri uffici o in locali idonei alla loro conservazione materiale adibiti ad archivio di deposito. Ciascuna UO deve provvedere al condizionamento dei documenti e al mantenimento del loro ordinamento.

12 Disposizioni finali

Le disposizioni contenute nel Manuale devono essere adottate a partire dal giorno successivo a quello della pubblicazione della delibera di approvazione all'Albo camerale informatico.

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

Il RGD, in attuazione del presente documento, ha il compito di:

a) proporre o redigere progetti speciali tendenti alla valorizzazione dei documenti della Camera di Commercio, alla conservazione, alla sicurezza dei locali di deposito e a quant'altro possa migliorare l'attività istituzionale inerente agli archivi;

b) proporre iniziative di formazione e aggiornamento professionale.

ELENCO ALLEGATI

1. GEDOC - Organigramma
2. Elenco metadati
3. Registro di emergenza
4. Piano della sicurezza

Organigramma GEDOC

- 1.1 AOO000
 - 1.1.1 Segretario Generale
 - 1.1.1.1 UFFICIO SEGRETERIA GENERALE
 - 1.1.1.2 SEGRETERIA PRESIDENZA
 - 1.1.1.3 SETTORE TURISMO E RELAZIONI ESTERNE
 - 1.1.1.4 SERVIZIO AFFARI GENERALI E PROTOCOLLO
 - 1.1.1.4.1 Affari generali - Protocollo
 - 1.1.1.4.2 Biblioteca
 - 1.1.1.5 DIR.SETTORI RAGIONERIA E BILANCIO / PROVVEDITORATO
 - 1.1.1.5.1 PROVVEDITORATO
 - 1.1.1.5.1.1 Ufficio Provveditorato
 - 1.1.1.5.1.2 Ufficio Gare
 - 1.1.1.5.1.3 UFFICIO POSTA
 - 1.1.1.5.2 RAGIONERIA E BILANCIO
 - 1.1.1.5.2.1 Ufficio Contabilita e Bilancio
 - 1.1.1.5.2.2 Tributi
 - 1.1.1.5.2.3 C.E.D.
 - 1.1.1.6 DIR.II: ATTIVITA PROMOZIONALI
 - 1.1.1.6.1 Istituto di Economia Internazionale
 - 1.1.1.6.2 Settore servizi alle attivita produttive e commerciali
 - 1.1.1.6.3 Settore Servizi Innovativi
 - 1.1.1.6.3.1 REC
 - 1.1.1.6.3.2 Borsa merci
 - 1.1.1.6.4 PROMOZIONE AGRICOLTURA E ARTIGIANATO
 - 1.1.1.6.5 Settore Internazionalizzazione
 - 1.1.1.6.5.1 Certificati di Origine
 - 1.1.1.6.6 Settore Logistica
 - 1.1.1.6.6.1 FLAG
 - 1.1.1.6.6.2 PROMOZIONE SETTORE MARITTIMO
 - 1.1.1.6.6.3 PROMOZIONE TRASPORTI
 - 1.1.1.6.7 SEZIONE CHIAVARI ED EVENTI ALLUVIONALI
 - 1.1.1.6.7.1 SEZIONE DI CHIAVARI
 - 1.1.1.6.7.2 UFFICIO ALLUVIONI
 - 1.1.1.6.7.2.1 Ristori covid
 - 1.1.1.6.7.3 PONTE MORANDI
 - 1.1.1.6.8 SETTORE LAVORO CREDITO USI E PROTESTI
 - 1.1.1.6.8.1 CREDITO
 - 1.1.1.6.8.2 Protesti
 - 1.1.1.6.8.3 USI

-  Ufficio orientamento al lavoro
-  DIR. III: SERVIZI ANAGRAFICI
-  SETTORE REGISTRO IMPRESE - ARTIGIANATO
 -  Albo Imprese Artigiane
 -  Ufficio Registro Imprese
 -  Ruolo Agenti e Rappresentanti di Commercio
-  SETTORE AMBIENTE E ABILITAZIONI SPECIALI
 -  UFFICIO AMBIENTE
 -  Pratiche automatiche
 -  m.u.d.
 -  Registro Pile
 -  Sottoprodotti
 -  Registro A E E
 -  UFFICIO ABILITAZIONI SPECIALI
 -  Registro F Gas
-  DIR.V: REGOLAZIONE DEL MERCATO
-  SETTORE SERVIZI REGOLAZIONE DEL MERCATO
 -  Camere Arbitrali - Usi - Conciliazione
-  UFFICIO SANZIONI AMMINISTRATIVE
-  RUOLI - ELENCHI
 -  MEDIATORI MARITTIMI
 -  PERITI ED ESPERTI SPEDIZIONIERI RACC. MARITT. PESATORI E STIMATORI
 -  RUOLO AGENTI DI AFFARI IN MEDIAZIONE
-  SETTORE INNOVAZIONE
 -  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
 -  Responsabile Protezione Dati
-  UFFICI CESSATI
 -  Albo Promotori Finanziari
 -  Uff. Panificazione

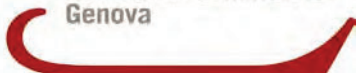
Documenti soggetti a registrazione particolare e relativi metadati (art.5, c.2, lett. e) DPCM 3 dicembre 2013)

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, Sottotipo, 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 appartenenza, 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 (Si/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



Camera di Commercio
Genova



REGISTRO DI PROTOCOLLO DI EMERGENZA

numero protocollo		data		
tipo	E/U	riservato	si	no
protocollo mittente				
modalità arrivo o partenza				
mittente o destinatario				
oggetto				
assegnatario				
altri assegnatari				
classifica				
Allegati n.				
descrizione allegati				
Note				
cod id protocollatore				

PIANO PER LA SICUREZZA INFORMATICA

Il Piano per la sicurezza del sistema di gestione informatica dei documenti è predisposto ai sensi dell'art. 3, comma 1, lett. g) del D.P.C.M. 3 dicembre 2013 e nel rispetto:

- dell'art. 32 del Regolamento (UE) 2016/679 (GDPR), che impone al Titolare del trattamento l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio;
- delle Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni, adottate con Circolare AgID n. 2 del 18 aprile 2017 e successivamente aggiornate in raccordo con il framework nazionale di cybersicurezza definito dall'Agenzia per la Cybersicurezza Nazionale (ACN) ai sensi del D.L. 14 giugno 2021, n. 82;
- delle disposizioni del D.Lgs. 30 giugno 2003, n. 196 (Codice Privacy) come novellato dal D.Lgs. 10 agosto 2018, n. 101;
- delle Linee Guida del Garante per la Protezione dei Dati Personali applicabili ai trattamenti effettuati dalle pubbliche amministrazioni.

Il Piano è redatto in coordinamento con il Responsabile della sicurezza, il Responsabile della conservazione, il Responsabile per la Transizione al Digitale e, previo parere obbligatorio, il Responsabile della Protezione dei Dati (DPO). Il piano è soggetto a revisione periodica, con cadenza almeno biennale o in occasione di modifiche organizzative, normative o tecnologiche rilevanti.

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, vale a dire il CLP – Centro ligure produttività, con sede presso la Camera di Genova in Via Boccardo. Rientrano nell'ambito sopradescritto anche i trattamenti gestiti dalla Azienda speciale 'WTC Genoa' – 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. Occorre segnalare inoltre che è in previsione il passaggio dei server camerali al cloud di Infocamere ScpA.

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 (Raee) 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.

Tali 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'incarico 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

Le credenziali di autenticazione ai sistemi che trattano dati personali devono rispettare i seguenti requisiti minimi:

- la lunghezza minima della password è di 12 caratteri; è incoraggiato l'uso di passphrase di lunghezza maggiore;
- deve contenere caratteri appartenenti ad almeno tre delle seguenti categorie: lettere maiuscole, lettere minuscole, cifre numeriche, caratteri speciali;
- non deve contenere l'identificativo utente (user-id), il nome o il cognome dell'utente, o sequenze ovvie (es. «password», «12345678», date di nascita);
- non deve essere identica alle ultime 5 password utilizzate;

- la sostituzione periodica obbligatoria della password non è di norma richiesta in assenza di indicatori di compromissione; è tuttavia obbligatoria al primo utilizzo, a seguito di reset da parte dell'amministratore, e in caso di sospetta compromissione;
- non deve essere comunicata ad altri utenti; la condivisione delle credenziali è vietata.

Autenticazione multi-fattore (MFA)

Per l'accesso ai sistemi che trattano dati personali, in particolare per gli accessi da remoto, per i sistemi di conservazione documentale e per i profili amministrativi, è obbligatorio l'utilizzo dell'autenticazione a più fattori (MFA). Il secondo fattore di autenticazione può essere realizzato mediante:

- applicazione di autenticazione (authenticator app) su dispositivo mobile registrato;
- codice OTP (One Time Password) generato da token fisico o software;
- certificato digitale su dispositivo in possesso esclusivo dell'utente.

Le modalità di implementazione della MFA sono definite dall'Ufficio CED in accordo con il Responsabile della sicurezza e comunicate agli utenti con adeguato anticipo rispetto all'attivazione.

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 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 all'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.

In conformità a quanto previsto dall'art. 32 del Regolamento (UE) 2016/679 (GDPR) e tenuto conto delle linee guida AgID in materia di sicurezza ICT, il Titolare ha adottato le seguenti misure tecniche e organizzative adeguate:

- 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 conformità al provvedimento del Garante del 27/11/2008 (modificato il 25/06/2009) e alle misure di sicurezza previste dall'art. 32 del Regolamento (UE) 2016/679, il Titolare ha individuato e nominato gli amministratori di sistema, provvedendo all'aggiornamento periodico dell'elenco. L'ultimo aggiornamento è stato effettuato in data 23.04.2026. Sono adottate misure di registrazione degli accessi logici ai sistemi gestiti dagli amministratori. 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 consentito lo svolgimento dell'attività lavorativa in modalità di lavoro agile (prevista dalla l.n.81/2017). Tale modalità permette al personale autorizzato di svolgere la prestazione lavorativa da remoto, utilizzando una piattaforma di condivisione approntata da Infocamere ScpA tramite un servizio VPN (Virtual Private Network), utilizzando strumenti informatici e telematici idonei e nel rispetto delle misure

organizzative, di sicurezza e di protezione dei dati adottate dall'Amministrazione. L'Ente ha fornito specifiche indicazioni in materia di salute e sicurezza sul lavoro, utilizzo delle dotazioni informatiche, protezione delle informazioni e corretta gestione degli ambienti di lavoro, al fine di garantire adeguati livelli di tutela per i lavoratori e per il patrimonio informativo dell'Amministrazione.

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 IC Rete 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 (modificato il 25/06/2009), 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 Administrator.
- 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 evidenzii malfunzionamenti od incongruenze nella gestione dei dati, gli incaricati del trattamento devono dare tempestiva comunicazione all'Ufficio CED, che provvederà a verificare gli stessi e 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 all'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 IC Rete.

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 filtering

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. "webfiltering" 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 prevenivano 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.