



**Ordine dei Dottori Commercialisti  
e degli Esperti Contabili di Roma**

# **MANUALE DI GESTIONE DOCUMENTALE**

**Approvato nella seduta di Consiglio del 21 settembre 2015  
Aggiornato nella seduta del 4 aprile 2016**

# Sommario

<b>1. PRINCIPI GENERALI E ORGANIZZATIVI .....</b>	<b>7</b>
1.1. PREMessa.....	7
1.2. AMBITO DI APPLICAZIONE DEL MANUALE .....	8
1.3. DEFINIZIONI E NORME DI RIFERIMENTO PRINCIPALI.....	8
1.5. IL RESPONSABILE PER LA TENUTA DEL PROTOCOLLO INFORMATICO, PER LA GESTIONE DEI FLUSSI DOCUMENTALI, DEGLI ARCHIVI E DELLA CONSERVAZIONE.....	10
1.5.1. IL DELEGATO PER LA TENUTA DEL PROTOCOLLO INFORMATICO.....	10
1.5.2. IL DELEGATO PER LA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI.....	10
1.6. UNITÀ RESPONSABILI DELLE REGISTRAZIONI DI PROTOCOLLO .....	11
1.7. RESPONSABILI DELL'ASSEGNAZIONE E DELLA GESTIONE DELLA DOCUMENTAZIONE.....	12
1.8. ATTI DI ORGANIZZAZIONE.....	12
1.9. POSTA ELETTRONICA CERTIFICATA (PEC) .....	13
1.10. FIRMA DIGITALE .....	13
1.11. FIRMA ELETTRONICA .....	13
1.12. DIRITTO DI ACCESSO E TUTELA DEI DATI PERSONALI.....	13
1.12.1. PRINCIPI GENERALI .....	13
1.12.2 IL DELEGATO PER LA CONSERVAZIONE .....	14
1.12.3. DIRITTO DI ACCESSO PER FINI AMMINISTRATIVI .....	15
1.12.4. L'ACCESSO CIVICO.....	15
1.12.5. DIRITTO DI CONSULTAZIONE PER RICERCA STORICO-SCIENTIFICA .....	15
1.12.6. TUTELA DEI DATI PERSONALI .....	15
<b>2. IL DOCUMENTO.....</b>	<b>16</b>
2.1. IL DOCUMENTO.....	16
2.2. IL DOCUMENTO AMMINISTRATIVO.....	16
2.2.1. IL DOCUMENTO AMMINISTRATIVO ANALOGICO .....	16
2.2.2. IL DOCUMENTO AMMINISTRATIVO INFORMATICO.....	16
2.3. DISTINZIONE DEI DOCUMENTI IN BASE ALLO STATO DI TRASMISSIONE .....	17
2.3.1. DOCUMENTI IN ARRIVO .....	17
2.3.2. DOCUMENTI IN PARTENZA .....	17
2.3.3. DOCUMENTI INTERNI .....	17
2.4. IL DOCUMENTO DELL'ORDINE: DEFINIZIONE E REGIME GIURIDICO .....	17



2.4.1. ELEMENTI CARATTERIZZANTI IL DOCUMENTO AMMINISTRATIVO IN PARTENZA .....	18
2.4.2. GESTIONE DELL'OGGETTO DEL DOCUMENTO .....	18
2.4.3. FORMAZIONE E GESTIONE DEL DOCUMENTO INFORMATICO IN PARTENZA O INTERNO .....	19
2.4.4. FORMAZIONE E GESTIONE DEL DOCUMENTO CARTACEO IN PARTENZA O INTERNO .....	19
2.4.5. VALIDITÀ DEL DOCUMENTO AMMINISTRATIVO IN ARRIVO .....	19

### **3. FLUSSI DI LAVORAZIONE DEI DOCUMENTI IN ARRIVO..... 20**

3.1. DOCUMENTO INFORMATICO RICEVUTO SU CASELLA PEC ISTITUZIONALE .....	20
3.1.1. DOCUMENTO RICEVUTO DI COMPETENZA DELL'ORDINE .....	20
3.1.2. DOCUMENTO RICEVUTO NON DI COMPETENZA DELL'ORDINE .....	21
3.2. DOCUMENTO INFORMATICO RICEVUTO SULLE ALTRE CASELLE PEC OPERATIVE E FUNZIONALI.....	21
3.2.1. DOCUMENTO DI COMPETENZA DELLA UO.....	21
3.2.2. DOCUMENTO DI COMPETENZA NON ESCLUSIVA DELLA UO .....	21
3.2.3. DOCUMENTO NON DI COMPETENZA DELLA UO.....	21
3.3. DOCUMENTO INFORMATICO RICEVUTO A MEZZO FAX .....	21
3.4. DOCUMENTO INFORMATICO RICEVUTO SU CASELLA E-MAIL CONVENZIONALE.....	22
3.4.1. DOCUMENTO RICEVUTO DI COMPETENZA DELLA UO .....	22
3.4.3. DOCUMENTO RICEVUTO DI COMPETENZA NON ESCLUSIVA DELLA UO .....	22
3.4.4. DOCUMENTO RICEVUTO NON DI COMPETENZA DELLA UO .....	22
3.5. DOCUMENTO INFORMATICO RICEVUTO SU SUPPORTO RIMUOVIBILE .....	22
3.6. DOCUMENTO INFORMATICO RICEVUTO TRAMITE SISTEMI TELEMATICI - SPORTELLO DIGITALE.....	22
3.7. DOCUMENTO ANALOGICO RICEVUTO PRESSO IL PROTOCOLLO E LE SEGRETERIE .....	23
3.8. ACCETTAZIONE DI DOCUMENTO ANALOGICO .....	23
3.9. ACCETTAZIONE DI DOCUMENTO ANALOGICO PRESSO LE UO.....	24
3.9.1. DOCUMENTO ANALOGICO DI COMPETENZA, ANCHE NON ESCLUSIVA, DELLA UO .....	24
3.9.2. DOCUMENTO ANALOGICO NON DI COMPETENZA DELLA UO.....	25
3.10. DOCUMENTI ANALOGICI CHE NECESSITANO DI TRATTAMENTO PARTICOLARE .....	25
3.10.1. DOCUMENTI NON SCANSIONABILI CONTESTUALMENTE ALLA RICEZIONE .....	25
3.10.2. DOCUMENTI RISERVATI O PERSONALI .....	25
3.10.3. ATTI GIUDIZIARI NOTIFICATI.....	25
3.10.4. ATTI RELATIVI A PROCEDURE DI GARA O AD OFFERTE .....	26
3.10.5. DOCUMENTI NON ATTINENTI ALLE ATTIVITÀ DELL'ORDINE .....	26
3.11. REGISTRAZIONE DI PROTOCOLLO E RELATIVA SEGNATURA .....	26
3.12. SMISTAMENTO E ASSEGNAZIONE ALLE UOP .....	26
3.13. CLASSIFICAZIONE E FASCICOLAZIONE .....	27

### **4. FLUSSI DI LAVORAZIONE DEI DOCUMENTI IN PARTENZA E A RILEVANZA INTERNA..... 27**



4.1. PREDISPOSIZIONE DEL DOCUMENTO IN PARTENZA E DEL DOCUMENTO INTERNO .....	27
4.2. APPROVAZIONE.....	28
4.3. REGISTRAZIONE DI PROTOCOLLO E RELATIVA SEGNAZIONE .....	28
4.4. INVIO DEL DOCUMENTO.....	28
4.5. MATERIALIZZAZIONE DEL DOCUMENTO INFORMATICO .....	29
4.5.1. SPEDIZIONE TRAMITE POSTA.....	29
4.5.2. SPEDIZIONE A MEZZO FAX .....	29
4.5.3. CONSEGNA A MANO .....	29
<b>5. PRODUZIONE DEL PROTOCOLLO INFORMATICO .....</b>	<b>30</b>
5.1. UNICITÀ DEL PROTOCOLLO .....	30
5.2. REGISTRO GIORNALIERO DI PROTOCOLLO.....	30
5.3. REGISTRAZIONE DI PROTOCOLLO .....	31
5.3.1. DOCUMENTI INFORMATICI .....	33
5.3.2. DOCUMENTI ANALOGICI E SUPPORTI RIMOVIBILI .....	33
5.4. LIVELLO DI RISERVATEZZA.....	33
5.5. SEGNAZIONE DI PROTOCOLLO DEI DOCUMENTI .....	34
5.5.1. DOCUMENTI INFORMATICI .....	34
5.5.2. DOCUMENTI ANALOGICI .....	34
5.6. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO .....	35
5.7. PROTOCOLLO DI EMERGENZA .....	35
5.8. DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E CASI PARTICOLARI DI REGISTRAZIONE.....	36
5.9. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO TRAMITE I SHAREDOC .....	36
5.10. CARATTERISTICHE DEL REGISTRO INFORMATICO DI PROTOCOLLO .....	36
5.10.1. RIFERIMENTO TEMPORALE DEL PROTOCOLLO .....	36
5.10.2. REGISTRO INFORMATICO DI PROTOCOLLO .....	36
5.10.3. TENUTA DEL REGISTRO GIORNALIERO DI PROTOCOLLO.....	36
5.11. DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO .....	37
<b>6. SISTEMA DI GESTIONE ARCHIVISTICA .....</b>	<b>37</b>
6.1. GENERALITÀ .....	37
6.2. MISURE DI TUTELA E VALORIZZAZIONE DELL'ARCHIVIO DELL'ORDINE .....	37
6.3. TITOLARIO DELL'ORDINE.....	37
6.4. CLASSIFICAZIONE DEI DOCUMENTI .....	38



6.5. FASCICOLAZIONE DEI DOCUMENTI .....	38
6.6. PIANO DI FASCICOLAZIONE .....	39
6.7. TIPOLOGIE E DURATA DEL FASCICOLO .....	39
6.7.1. FASCICOLO “PROCEDIMENTO 241” E FASCICOLO “ISTRUTTORIO” .....	39
6.7.2. FASCICOLO DI “ATTIVITÀ” .....	40
6.7.3. FASCICOLO DI “PERSONA FISICA O GIURIDICA” .....	40
6.7.4. FASCICOLO “STANDARD” .....	41
6.8. APERTURA DEL FASCICOLO .....	41
6.9. OGGETTO DEL FASCICOLO .....	41
6.10. IL SOTTOFASCICOLO .....	41
6.11. CHIUSURA DEL FASCICOLO.....	42
<b>7. GESTIONE IN SICUREZZA DEI DOCUMENTI INFORMATICI .....</b>	<b>42</b>
7.1. PRINCIPI GENERALI .....	42
7.2. MISURE GENERALI DI SICUREZZA PER LA GESTIONE DOCUMENTALE .....	42
7.3. FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA .....	43
7.4. GESTIONE DEI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA.....	43
7.4.1. COMPONENTE FISICA .....	43
7.4.2. COMPONENTE LOGICA E INFRASTRUTTURALE.....	43
7.4.3. GESTIONE PERMESSI PER ASSEGNAZIONI .....	44
7.4.4. GESTIONE DELLA RISERVATEZZA .....	44
7.4.5. GESTIONE DEI TRACCIAMENTI .....	44
7.5. TRASMISSIONE DEI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA .....	45
7.6. ACCESSO AI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA.....	45
7.6.1. PROFILI DI ACCESSO .....	46
7.6.2. MODALITÀ DI GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO .....	46
7.6.3. UTENTI INTERNI .....	46
7.6.4. UTENTI ESTERNI .....	46
7.7. POLITICHE DI SICUREZZA ADOTTATE DALL’ORDINE .....	47
7.8. MANUTENZIONE ORDINARIA ED AGGIORNAMENTI.....	47
7.9. GESTIONE DI EVENTI ECCEZIONALI .....	47
<b>8. CONSERVAZIONE DEI DOCUMENTI INFORMATICI.....</b>	<b>48</b>
8.1 AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE .....	48
8.2 COMPITI DEL RESPONSABILE DELLA CONSERVAZIONE .....	48



8.3 TIPOLOGIE DOCUMENTALI E RELATIVE TEMPISTICHE DI INVIO IN CONSERVAZIONE .....	49
<b><u>9. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE .....</u></b>	<b><u>49</u></b>
9.1. MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO.....	49
9.2. PUBBLICITÀ DEL MANUALE .....	50
9.3. ENTRATA IN VIGORE DEL MANUALE .....	50
<b><u>ADDENDA .....</u></b>	<b><u>51</u></b>



## **1. PRINCIPI GENERALI E ORGANIZZATIVI**

### **1.1. PREMessa**

Il Codice dell'Amministrazione Digitale-CAD (d.lgs. 7 marzo 2005, n. 82, come successivamente modificato) promuove l'innovazione nelle pubbliche amministrazioni mediante la razionalizzazione delle strutture organizzative e l'informatizzazione dei procedimenti e delle attività, nel rispetto dei principi di trasparenza e di accesso alle informazioni da parte dei cittadini.

Il CAD enuncia principi e modalità operative a cui le amministrazioni pubbliche devono ispirarsi nei rapporti interni ed esterni, funzionali al perseguimento di adeguati livelli di qualità nell'erogazione dei servizi ai cittadini e alle imprese.

Ai fini di garantire una corretta ed efficiente gestione documentale, il DPCM del 3 dicembre 2013 - recante "Regole tecniche per il protocollo informatico", adottato ai sensi dell'art. 71 del CAD - prevede l'obbligo per le pubbliche amministrazioni di "adottare il manuale di gestione di cui all'articolo 5, su proposta del Responsabile della gestione documentale" (art. 3).

Il presente Manuale di gestione persegue una duplice finalità, entrambe coerenti con il quadro normativo di riferimento: disciplinare il sistema di gestione documentale, a partire dalla fase di protocollazione della corrispondenza in ingresso, in uscita e interna; rappresentare le funzionalità disponibili ai soggetti che a diverso titolo interagiscono con l'Ordine.

Il Manuale è destinato alla più ampia diffusione e conoscenza, anzitutto interna, mirando a fornire istruzioni esaustive per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Pertanto, esso si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti ed anche ai soggetti esterni che si relazionano con l'Ordine.

Nello specifico, il Manuale disciplina:

- la gestione flussi documentali digitali e cartacei in rapporto con il protocollo informatico e il sistema di conservazione ;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del Titolario di classificazione;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

Stante la sua natura - di documento operativo interno ma anche da rendere pubblico all'esterno - esso assolve il duplice ruolo di strumento di supporto per i processi operativi e decisionali interni e di documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

Il Manuale va inteso, dunque, quale "atto di organizzazione" che descrive le varie fasi operative del sistema di gestione del protocollo informatico, dei flussi documentali e degli archivi, individuando per ogni azione o processo i rispettivi livelli di esecuzione, responsabilità e controllo, in una visione d'insieme che va, senza soluzioni di continuità, dalla protocollazione del documento, alla sua gestione, archiviazione e fascicolazione, sino alla conservazione ai sensi di legge.

Ciò essendo, il Manuale specifica ruoli e funzioni delle strutture organizzative e dei soggetti coinvolti nel processo di gestione documentale, inteso come insieme strutturato di attività complesse riguardanti l'intero ciclo operativo dell'Ordine.



## 1.2. AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma d), del citato DPCM del 3 dicembre 2013 recante "Regole tecniche per il protocollo informatico".

Per quanto sopra rilevato, esso disciplina le attività di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti; i flussi documentali da e verso l'esterno e interni; le procedure di gestione archivistica della documentazione in relazione ai procedimenti amministrativi e alle attività proprie dell'Ordine, ivi inclusa la procedura interna di gestione dei documenti.

La gestione documentale dell'Ordine si fonda sulla compenetrazione di tre principi archivistici:

1. la registrazione di protocollo del documento che fa fede, a ogni effetto, del ricevimento e della spedizione di un documento;
2. la classificazione del documento, anche non protocollato, che lo dota della collocazione logico-funzionale nell'Archivio;
3. la fascicolazione del documento, protocollato o non protocollato, che attesta la sua effettiva gestione nell'ambito di un procedimento amministrativo o di un'attività.

## 1.3. DEFINIZIONI E NORME DI RIFERIMENTO PRINCIPALI

Ai fini del presente Manuale si intende per:

- **CAD**: il decreto legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale e successive modificazioni.
- **Regole tecniche per la conservazione**: il decreto del Presidente del Consiglio dei Ministri 10 del 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005".
- **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 ,
- **Testo Unico**: il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Si riportano, di seguito, gli acronimi e i termini utilizzati più frequentemente:

- **AOO**: Area Organizzativa Omogenea, quale 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.
- **Campo**: parte della scheda documentale per l'inserimento di una specifica informazione o metadato relativo al documento informatico.
- **Delegati**: personale dell'Ordine incaricato formalmente dal RGD per l'espletamento di funzioni previste dalla normativa vigente in materia di amministrazione digitale.
- **iShareDoc**: sistema centrale e integrato di gestione documentale e protocollo informatico; applicativo acquisito dall'Ordine per implementare il servizio integrato di protocollo informatico e gestione dei flussi documentali.





- **Ordine:** Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma.
- **MdG:** Manuale di Gestione del protocollo informatico, dei documenti e degli archivi.
- **OdS:** Ordine di Servizio.
- **PA:** Pubblica Amministrazione.
- **PEC:** Posta Elettronica Certificata.
- **RdP:** Responsabile del Procedimento - il dipendente o il Consigliere dell'Ordine che assume su di sé la responsabilità dell'esecuzione degli adempimenti amministrativi relativi a un procedimento.
- **RdU:** Responsabile di Ufficio, da intendersi quest'ultimo quale UO.
- **RdUNC:** Responsabile di Ufficio non Coordinato, parimenti da intendersi quale UO e identificato nel Direttore dell'Ordine.
- **RGD:** Responsabile della gestione documentale, ovvero della tenuta del Protocollo informatico, della gestione dei flussi documentali, nonché degli archivi e della conservazione.
- **Scheda documentale:** insieme di dati e metadati associati ad uno specifico documento, con eventuali relativi allegati, che ne tipizzano gli elementi informativi, utili in fase di protocollazione, fascicolazione, conservazione, gestione e ricerca.
- **UOP:** Unità Organizzative di registrazione di Protocollo - identificano gli uffici che svolgono attività di registrazione di protocollo.
- **UO:** ai sensi della normativa di riferimento, corrisponde alla Unità Organizzativa Responsabile e di Riferimento – vale a dire un insieme di uffici o un ufficio che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione unitarie e coordinate.
- **UP:** Unità di Protocollo - è la principale UOP, funzionalmente allocata nell'ufficio Affari Generali e Protocollo.

Per un elenco completo delle disposizioni rilevanti si veda A1 – Normativa di riferimento e bibliografia.

Per il Glossario si veda A2 – Glossario.

Per un elenco completo di abbreviazioni, sigle e acronimi si veda A3 – Abbreviazioni, sigle e acronimi dell'Ordine.

#### **1.4. MODELLI ORGANIZZATIVI**

Sotto il profilo normativo e archivistico, una AOO può essere definita come un insieme di risorse umane e strumentali dotate di propri organi di governo e di gestione per adempiere a determinate funzioni primarie. Di conseguenza una AOO usufruisce, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali.

Una UO rappresenta, invece, un sottoinsieme di una AOO, vale a dire un complesso di risorse umane e strumentali cui sono affidate una o più competenze omogenee, nel cui ambito i dipendenti assumono la responsabilità della gestione di procedimenti amministrativi e attività.

Ai fini del presente Manuale, l'Ordine individua un'unica AOO denominata Ordine, composta dall'insieme delle UO da cui è caratterizzato il relativo assetto organizzativo e funzionale (A4 – Scheda dell'Ordine).



Le UO che, alla data di adozione del presente Manuale, afferiscono alla AOO sono riportate in A5 – UO dell’Ordine che potrà formare oggetto di modifiche ed integrazioni per effetto di successivi interventi sulla struttura organizzativa interna.

### **1.5. IL RESPONSABILE PER LA TENUTA DEL PROTOCOLLO INFORMATICO, PER LA GESTIONE DEI FLUSSI DOCUMENTALI, DEGLI ARCHIVI E DELLA CONSERVAZIONE**

Il “Responsabile per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi” nonché di “Responsabile della conservazione”, ai sensi della normativa di riferimento, è stato individuato nella persona del direttore dell’Ordine.

È in facoltà del Responsabile di avvalersi della delega di funzioni a dipendenti dell’Ordine in possesso dei necessari requisiti di competenza e professionalità tecnica; facoltà di cui il Responsabile si è avvalso, ai sensi e per gli effetti di cui alla normativa vigente, nei termini di seguito riportati.

#### **1.5.1. Il delegato per la tenuta del protocollo informatico**

I compiti del delegato per la tenuta del protocollo informatico sono:

- garantire il rispetto delle disposizioni normative e delle procedure durante le operazioni di registrazione e di segnatura di protocollo;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- conservare le copie di salvataggio del registro giornaliero di protocollo e del registro di emergenza in sistemi diversi da quello in cui opera il sistema i ShareDoc;
- aprire e chiudere il registro di protocollazione di emergenza;
- curare le attività di registrazione di protocollo affinché, in caso di guasti o anomalie, ne sia ripristinata la funzionalità entro ventiquattrore dal blocco e, comunque, nel più breve tempo possibile.

Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

#### **1.5.2. Il delegato per la gestione dei flussi documentali e degli archivi**

I compiti del delegato alla gestione dei flussi documentali e degli archivi, con riferimento alla gestione dell’“archivio corrente” e/o “archivio in formazione”, sono:

- garantire il funzionamento degli strumenti e dell’organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso ai documenti, amministrativi e non, e le attività di gestione degli archivi;
- abilitare gli addetti dell’Ordine all’utilizzo del protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, registrazione, modifica, etc.);
- curare la redazione e l’aggiornamento del Titolario dell’Ordine, del Piano di fascicolazione e degli altri strumenti archivistici previsti;
- predisporre lo schema del Manuale di gestione di cui all’art. 5 delle Regole tecniche per il protocollo;
- predisporre il piano di visibilità e accesso in sicurezza relativo alla formazione, alla gestione, alla trasmissione, all’interscambio, all’accesso, alla conservazione dei documenti nel rispetto delle



misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, con i preposti ai sistemi informativi e con il responsabile del trattamento dei dati personali di cui al suddetto decreto;

- definire e assicurare criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione, nonché di comunicazione interna, ai sensi dell'art. 50, comma 4, del testo unico.

Con riferimento ai documenti contenenti informazioni di carattere particolarmente riservato (c.d. documenti L2), il delegato è autorizzato ad accedere, ai fini della gestione del sistema, ai metadati di tali documenti ed alle PEC. Ove necessario, è autorizzato ad accedere anche ai documenti di cui trattasi, previa richiesta al responsabile della sicurezza, che traccia tali accessi.

Con riferimento all'archivio di "deposito" per la documentazione su supporto analogico, i compiti del delegato sono:

- individuare, d'intesa con le UO, le procedure di trasferimento delle unità archivistiche relative a procedimenti amministrativi e attività conclusi, curando la redazione degli elenchi di versamento e di consistenza, nonché degli altri strumenti archivistici;
- effettuare le operazioni di valutazione dei documenti ai fini della conservazione, curando la redazione e l'aggiornamento del prontuario e del massimario di selezione;
- curare le procedure di scarto e di riordino della documentazione;
- curare la movimentazione dei fascicoli, delle aggregazioni e delle serie documentarie;
- permettere l'esercizio del diritto di accesso, ponendo attenzione alla tutela dei dati personali e sensibili.

Con riferimento all'archivio "storico" per la documentazione su supporto analogico, i compiti del delegato sono:

- individuare le procedure di versamento delle unità archivistiche relative a procedimenti amministrativi e attività conclusi e selezionati per la conservazione permanente.

Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

## **1.6. UNITÀ RESPONSABILI DELLE REGISTRAZIONI DI PROTOCOLLO**

Nell'Ordine il sistema di protocollazione è:

- *unico a livello istituzionale*, cioè tutte le UO e gli utenti abilitati accedono al sistema iShareDoc per le operazioni di protocollazione;
- *distribuito per la corrispondenza in entrata e in uscita*, essendo previste più UOP per la protocollazione dei documenti in entrata e in uscita.

Nello specifico, le UO dell'Ordine svolgono i compiti di UOP principale dell'Ordine per la corrispondenza in entrata e in uscita di competenza e la UO Protocollo di UOP secondaria per la corrispondenza in entrata e in uscita.

Da un punto di vista operativo la distribuzione, le abilitazioni e le attività di protocollazione della corrispondenza in entrata e in uscita seguono le indicazioni stabilite nel presente Manuale e sono sottoposte, anche per ciò che concerne la corretta esecuzione dei compiti previsti, al controllo del delegato alla tenuta del protocollo informatico.



### **1.7. RESPONSABILI DELL'ASSEGNAZIONE E DELLA GESTIONE DELLA DOCUMENTAZIONE**

I RdU e il RdUNC, sono responsabili dell'assegnazione e della gestione della documentazione di competenza della UO a cui sono preposti. Al fine di assicurare la continuità operativa, in caso di assenza o impedimento del Responsabile opera in sua vece il sostituto nominato dal Direttore.

### **1.8. ATTI DI ORGANIZZAZIONE**

L'Ordine, come già sopra rilevato, è identificato come un'unica AOO.

In data 24/09/2009 è stata istituita la casella di Posta Elettronica Certificata istituzionale dell'Ordine.

In data 17/11/2009 l'Ordine è stato accreditato dall'Indice delle Pubbliche Amministrazioni - IPA come previsto dall'art. 57-bis del CAD. La relativa scheda è consultabile all'indirizzo:

[http://www.indicepa.gov.it/ricerca/n-dettaglioamministrazione.php?cod\\_amm=ODCECRM](http://www.indicepa.gov.it/ricerca/n-dettaglioamministrazione.php?cod_amm=ODCECRM)

Con disposizione del Consiglio dell'Ordine del 21 settembre 2015 è stato approvato il Titolario di classificazione.

Con delibera del Consiglio dell'Ordine del 21 settembre 2015 il Direttore dell'Ordine è stato, come già sopra anticipato, nominato "Responsabile per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi", nonché "Responsabile della conservazione".

In data 21 settembre 2015 tale Responsabile si è avvalso della delega di funzioni a dipendenti dell'Ordine in possesso dei necessari requisiti di competenza e professionalità tecnica.

Il sistema di gestione documentale dell'Ordine denominato iShareDoc, comprensivo del protocollo informatico, fondato sull'integrazione delle tecnologie digitali per l'intero ciclo di gestione del documento e dell'archivio informatico a rilevanza sia interna che esterna, è divenuto operativo a partire dal 1° luglio 2015.

A decorrere da tale data è stato sostituito il protocollo informatico e il sistema di gestione informatica dei documenti e degli archivi, ferma restando l'esigenza di registrazioni specifiche quali il registro degli affari trattati dall'OCC.

Dalla data del 1° ottobre 2015:

- la produzione di documenti originali su supporto cartaceo sarà progressivamente sostituita da documentazione ufficiale – sia interna sia indirizzata a soggetti esterni - prodotta in formato digitale e sottoscritta con firma digitale;
- la documentazione in formato cartaceo è acquisita via scanner, assegnata e trattata in formato digitale, eccezion fatta per i documenti che dovessero richiedere un loro trattamento solo su supporto fisico e i documenti per i quali non si prevede la scansione, secondo la casistica descritta nel presente Manuale;
- la documentazione ricevuta e prodotta nell'ambito dell'attività istituzionale è classificata secondo il Titolario di classificazione e fascicolata conformemente al "Piano di Fascicolazione" dell'Ordine (Allegato3 – Piano di Classificazione e Fascicolazione archivistica);
- la Posta Elettronica Certificata (PEC) è il vettore privilegiato di relazioni con l'esterno; pertanto, nel caso in cui il destinatario disponga di una casella PEC risultante da pubblici elenchi, ovvero accessibile alla pubblica amministrazione, ogni comunicazione formale al soggetto stesso è veicolata tramite tale casella;



- l’archiviazione dei documenti avviene in conformità alla normativa in tema di archiviazione corrente e sistema di conservazione, nonché in base alle disposizioni indicate nel presente Manuale;
- gli scambi formali di documenti tra UO dell’Ordine avvengono attraverso caselle email che saranno progressivamente implementate nella piattaforma iShareDoc;
- la documentazione digitale informatica, non necessariamente protocollata, è inserita nella piattaforma iShareDoc nei fascicoli di pertinenza ed eventualmente registrata in appositi registri”;
- la documentazione riguardante la pubblicità, la trasparenza e la diffusione di atti e informazioni da parte dell’Ordine, ovvero la pubblicazione sul relativo sito, è gestita e archiviata mediante la piattaforma iShareDoc in appositi registri.

### **1.9. POSTA ELETTRONICA CERTIFICATA (PEC)**

L’Ordine utilizza la PEC quale sistema gestionale e di comunicazione, ai sensi del CAD, 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 dell’Ordine è la seguente: [presidenza@pecodcec.roma.it](mailto:presidenza@pecodcec.roma.it).

La casella PEC istituzionale è utilizzabile sia per la trasmissione che per la ricezione.

In sede di trasmissione la casella è configurata per l’invio ad altri indirizzi PEC, per i quali si riceveranno le ricevute di consegna, ovvero a indirizzi di posta elettronica non certificata, per i quali non si riceveranno le ricevute di consegna.

In ricezione la casella è configurata per l’accettazione da parte dei soli indirizzi PEC.

Ciascun Ufficio è dotato di una propria casella PEC.

In presenza di comprovate specifiche esigenze operative possono essere rilasciate “caselle funzionali” dedicate.

L’elenco completo delle PEC dell’Ordine è riportato in A6 – Elenco PEC.

### **1.10. FIRMA DIGITALE**

L’Ordine utilizza la firma digitale per l’espletamento delle attività istituzionali e gestionali con la finalità, ai sensi del CAD, di rendere manifesta e di verificare la provenienza e l’integrità di un documento informatico o di un insieme di documenti informatici.

L’accreditamento presso l’Ente Certificatore (Certification Authority) è gestito dall’Ufficio Sistemi Informativi dell’Ordine.

Il rappresentante legale dell’Ordine e i responsabili dei procedimenti sono muniti di firma digitale.

### **1.11. FIRMA ELETTRONICA**

In conformità alla normativa vigente in materia di amministrazione digitale, le credenziali di accesso costituiscono la “**firma elettronica**” dell’utente che utilizza il sistema e qualsiasi azione e attività svolta in iShareDoc costituisce atto valido ai fini amministrativi.

### **1.12. DIRITTO DI ACCESSO E TUTELA DEI DATI PERSONALI**

#### **1.12.1. Principi generali**

Le procedure amministrative e il sistema iShareDoc sono implementati nel rispetto delle norme dettate in tema di diritto di accesso e di protezione dei dati personali e sensibili.



In particolare, i dipendenti, nell'esercizio delle proprie funzioni, sono tenuti all'osservanza dei doveri e degli obblighi previsti dalla normativa di riferimento, a non trarre profitto personale o a procurare danno a terzi e all'Ordine dalla conoscenza di fatti e documenti (cfr. A1 – Normativa di riferimento e bibliografia).

Ciascun dipendente può richiedere, relativamente ai documenti e alle informazioni presenti nell'archivio dell'Ordine, la consultazione di documenti relativi a procedimenti e attività di propria competenza ovvero di carattere generale (delibere, disposizioni, etc.) o anche singoli dati e informazioni ricavabili dai documenti o da banche dati, necessari in funzione del procedimento amministrativo o dell'attività svolta.

### **1.12.2 Il delegato per la conservazione**

Il delegato alla conservazione:

- a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- g) 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;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- j) 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;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.



Con riferimento ai documenti riportanti informazioni di carattere particolarmente riservato (c.d. documenti L2), il delegato è autorizzato ad accedere, ai fini della gestione del sistema, ai metadati dei documenti L2 ed alle PEC. Ove necessario, è autorizzato ad accedere anche ai documenti di cui trattasi, previa richiesta al responsabile della sicurezza, che traccia tali accessi. Il delegato si avvale di sostituti in caso di sua assenza o impedimento.

#### **1.12.3. Diritto di accesso per fini amministrativi**

In conformità alla normativa vigente, l'Ordine riconosce e disciplina il diritto di accesso e la consultazione per fini amministrativi da parte di terzi degli atti, dei fascicoli e dei documenti amministrativi formati o comunque rientranti nella sua disponibilità.

Con delibera del 27 gennaio 2014, l'Ordine ha approvato il Regolamento generale sui procedimenti amministrativi dell'Ordine, ai sensi della legge 7 agosto 1990, n. 241 e successive modificazioni.

Il Regolamento è pubblicato sul sito dell'Ordine.

Per l'esercizio del diritto di accesso ai documenti è previsto che il soggetto di norma presenti richiesta formale anche tramite PEC.

#### **1.12.4. L'accesso civico**

È il diritto riconosciuto a qualunque cittadino di richiedere documenti, informazioni e dati, oggetto di pubblicazione obbligatoria ai sensi della normativa vigente in materia di Trasparenza (D.lgs n. 33 del 14 marzo 2013), nei casi in cui l'amministrazione pubblica interessata non li abbia pubblicati sul proprio sito web istituzionale.

#### **1.12.5. Diritto di consultazione per ricerca storico-scientifica**

Allo stato non è istituito l'archivio storico dell'Ordine e non è disciplinata la consultazione di documenti da parte di terzi per finalità di ricerca storico-scientifica.

#### **1.12.6. Tutela dei dati personali**

L'Ordine, in qualità di ente a cui sono riconducibili i dati di protocollo e quelli personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza, dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti aventi rilevanza interna ed esterna.

Le regole e le modalità operative stabilite dall'Ordine per la sicurezza dei dati sono riportate nel *Documento Programmatico sulla Sicurezza dei dati personali ai sensi del D. Lgs. n. 196/2003*

In relazione alla protezione dei dati personali trattati, l'Ordine provvede a ottemperare a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.





I dati relativi al corrispondente (mittente o destinatario) sono archiviati e implementati per le sole parti essenziali e coerenti con l'attività di registrazione di protocollo, in ossequio al principio di necessità del trattamento dei dati personali previsto dall'art. 3 del decreto legislativo 30 giugno 2003 n. 196.

## **2. IL DOCUMENTO**

### **2.1. IL DOCUMENTO**

Ogni atto compiuto, per essere tramandato e avere rilevanza come fonte di prova, di attestazione o di semplice vademecum delle proprie attività, deve essere riprodotto su un documento.

Per documento si intende, dunque, una cosa (i.e., una *res*) idonea a ricevere, conservare, trasmettere la rappresentazione, comunque realizzata, del contenuto di atti, stati, fatti e qualità.

In ambito amministrativo, per atto comunemente si intende un evento riconducibile ad una pubblica amministrazione, avente tipicamente rilevanza esterna e posto in essere nell'esercizio della propria attività istituzionale, sostanziandosi in una manifestazione di volontà, di scienza, di valutazione o altro, a cui sono associati gli effetti previsti dalla legge e rappresentato in uno o più documenti.

La gestione documentale di una pubblica amministrazione ha riguardo ai documenti prodotti o acquisiti nello svolgimento delle relative funzioni istituzionali. Tali documenti, tra loro connessi da vincolo originario, necessario e determinato, vanno a costituire l'archivio dell'amministrazione.

### **2.2. IL DOCUMENTO AMMINISTRATIVO**

Ai sensi dell'articolo 22 comma 1, lettera d, della legge n. 241/1990, per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica, informatica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale.

#### **2.2.1. Il documento amministrativo analogico**

Il documento amministrativo analogico è la rappresentazione, mediante dati continui memorizzati su un supporto fisico, del contenuto di atti, fatti o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora.

Il documento analogico il cui contenuto è memorizzato su supporto cartaceo è leggibile senza l'ausilio di strumenti tecnologici.

#### **2.2.2. Il documento amministrativo informatico**

Il documento amministrativo informatico è la rappresentazione, mediante dati binari associati a un formato, del contenuto di atti, fatti o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora.

Il documento informatico è memorizzato su un supporto fisico che può essere di vari tipi (CDROM, DVD, disco rigido, memorie a stato solido, etc.) Ed è leggibile solo mediante l'ausilio di strumenti tecnologici.





### **2.3. DISTINZIONE DEI DOCUMENTI IN BASE ALLO STATO DI TRASMISSIONE**

In base allo stato di trasmissione i documenti si distinguono in:

- documenti in arrivo (mittente esterno, destinatario interno);
- documenti in partenza (mittente interno, destinatario esterno);
- documenti interni, cioè scambiati tra UO (mittente interno, destinatario interno).

#### **2.3.1. Documenti in arrivo**

Per documenti in arrivo si intendono i documenti acquisiti dall'Ordine nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

#### **2.3.2. Documenti in partenza**

Per documenti in partenza si intendono i documenti di rilevanza informativa e/o giuridicoprobativa prodotti dall'Ordine nell'esercizio delle proprie funzioni e indirizzati a un diverso soggetto pubblico o privato.

#### **2.3.3. Documenti interni**

Per documenti interni si intendono i documenti scambiati tra UO dell'Ordine.

Essi possono essere distinti, nel rispetto del principio di autonomia istruttoria nella valutazione degli stessi, in:

- documenti di preminente carattere informativo;
- documenti di preminente carattere giuridico-probatorio.

I documenti interni di preminente carattere informativo sono, in genere, memorie, appunti, comunicazioni e documenti di lavoro scambiati tra UO o tra dipendenti che di norma non sono protocollati.

Al fine di mantenere aggiornato e completo il fascicolo analogico o informatico, è necessario registrare questa tipologia di documenti interni nei fascicoli di pertinenza.

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti al fine di documentare fatti, stati o qualità inerenti all'attività svolta e alle azioni amministrative intraprese, ovvero qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi; in quanto tali, essi sono protocollati secondo le disposizioni previste nel Manuale e fascicolati con gli altri documenti nel fascicolo di pertinenza.

### **2.4. IL DOCUMENTO DELL'ORDINE: DEFINIZIONE E REGIME GIURIDICO**

Per documento dell'Ordine si intende ogni documento prodotto o acquisito dall'Ordine nello svolgimento della propria attività istituzionale e/o nell'esercizio delle proprie funzioni.

I documenti dell'Ordine sono prodotti e gestiti mediante sistemi informatici o analogici, come previsto dalla vigente normativa. La scheda documentale del sistema iShareDoc è parte integrante del documento informatico prodotto dall'Ordine.

A norma di legge, tutti i documenti dell'Ordine sono inalienabili.

Inoltre, i documenti, i fascicoli e l'archivio dell'Ordine nel suo complesso sono sottoposti alle tutele e alle garanzie previste dalla legge. Non è, pertanto, possibile eliminare i documenti dall'archivio se non tramite procedura di selezione legale dei documenti.



#### **2.4.1. Elementi caratterizzanti il documento amministrativo in partenza**

Indipendentemente dal supporto sul quale è memorizzato, il documento in partenza è redatto rispettando:

- l'impostazione generale dei documenti dell'Ordine;
- gli standard redazionali previsti per la singola tipologia di documento.

Secondo le modalità indicate nella normativa interna, il documento in partenza utilizza il formato documentale che prevede l'intestazione dell'Ordine completa per la sola prima pagina; abbreviata per le pagine successive alla prima.

I documenti in partenza devono inoltre riportare, ove disponibili, le seguenti informazioni:

- simbolo e denominazione ufficiali dell'Ordine;
- numero e data di protocollo;
- numero e data di registrazione, in caso di registrazione in apposito repertorio o registro;
- mezzo di spedizione (raccomandata a.r., posta elettronica, telefax, telematico, etc.);
- UO mittente;
- data del documento (luogo, giorno, mese, anno), ove necessario;
- dati del destinatario o dei destinatari (indirizzo completo, numeri di telefono, telefax, indirizzo di posta elettronica);
- numero di riferimento a un procedimento/fascicolo precedente o corrente;
- oggetto del documento;
- testo del documento;
- firma o sigla del legale rappresentante e/o del RdP e/o di, RdUNC, e/o RdU;
- numero e descrizione degli allegati;
- dati dell'Ordine (indirizzo completo, numeri di telefono e telefax, indirizzo istituzionale di posta elettronica);
- numero di pagina.

Il documento sprovvisto dei requisiti disponibili non può essere elaborato e, laddove ricevuto dalle Segreterie o dal Protocollo per le rispettive competenze di protocollazione e di invio, deve essere restituito all'istruttore o alla UO mittente con le indicazioni del caso.

Solo i documenti sottoscritti da quanti sono a ciò autorizzati da disposizioni generali o particolari possono essere registrati come corrispondenza ufficiale dell'Ordine.

Sono incaricati della verifica dei requisiti per l'invio di documenti all'esterno:

- il Responsabile di UO, ovvero il personale delle UO;
- il personale delle UO coinvolto nella redazione dei documenti;
- il personale con funzioni di Protocollo;
- il RGD e suoi delegati.

Per i documenti analogici su supporto cartaceo sono utilizzati, di norma, fogli bianchi del formato A4.

#### **2.4.2. Gestione dell'oggetto del documento**

Per un'efficace gestione documentale, sia nella fase corrente che in quella di ricerca e recupero delle informazioni, è consigliata l'adozione da parte di tutto il personale dell'Ordine di alcune



regole per la normalizzazione del campo “Oggetto” delle schede documentali iShareDoc e del relativo documento principale, al fine di definire un archivio razionale e usabile.

A tal riguardo si rimanda ai dettagli operativi riportati nel documento – Gestione del campo Oggetto della scheda documentale, in corso di predisposizione.

#### **2.4.3. Formazione e gestione del documento informatico in partenza o interno**

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

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file: comunemente è identificato attraverso l'estensione del file, pur considerando altri strumenti tecnici per l'identificazione e l'interpretazione del formato.

Le tipologie di formato principali adottate e gestite sono:

- Testi/documenti : PDF, PDF/A, DOC, DOCX, HTML, RTF, TXT
- Documenti con firma digitale : PDF/A, PDF, P7M
- Calcolo : XLS, XLSX
- Immagini : GIF, JPG, BMP, TIF
- Suoni : MP3, WAV
- Video : MPG, MPEG, AVI, WMV
- Archiviazione e Compressione : ZIP, GZ, GZIP, 7Z, NSF, PST
- E-mail : EML, SMTP/MIME
- Presentazione : PPTX, PPT, PPS
- Dati strutturati : CSV, XML (con relativi file interpretativi)

In particolare, per la creazione e formazione dei documenti si usano i formati DOCX, DOC, PDF.

Per il consolidamento del documento, cioè per la procedura di definizione di un documento originale, inteso quale definitivo, perfetto e autentico negli elementi sostanziali e formali, il documento deve essere firmato digitalmente e successivamente protocollato nel Registro di “Protocollo Ufficiale” ovvero archiviato in altro Registro dedicato a specifiche tipologie di documenti interni.

Nell'ambito dei formati dei file trattati non sono ammessi, o sono rimossi, codici integrati quali le cd. “macro” o cifrature dei contenuti, soprattutto per le finalità di conservazione digitale.

#### **2.4.4. Formazione e gestione del documento cartaceo in partenza o interno**

Il documento amministrativo cartaceo può essere prodotto in maniera tradizionale (come a esempio una lettera scritta a mano) ovvero con strumenti informatici (ad esempio una lettera prodotta tramite un text editor) e poi stampata. In quest'ultimo caso si definisce originale il documento cartaceo, nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia indicato al paragrafo 2.4.1., stampato su carta intestata e dotato di firma autografa.

#### **2.4.5. Validità del documento amministrativo in arrivo**

Sono considerati validi e gestibili direttamente i seguenti tipi di documento:

- *documenti analogici;*



- *documenti informatici* ricevuti su caselle PEC dell’Ordine e provenienti da caselle PEC, anche se privi della firma digitale;
- *documenti informatici* ricevuti tramite sistemi telematici (ad es. comunicazioni di variazioni dati da parte degli Iscritti).

Per i documenti informatici in arrivo, di norma, sono trattati i medesimi formati del documento informatico in partenza o interno.

### **3. FLUSSI DI LAVORAZIONE DEI DOCUMENTI IN ARRIVO**

Di seguito sono descritti i flussi di lavorazione dei documenti dell’Ordine, ricevuti dall’esterno o prodotti all’interno, se di preminente carattere giuridico-probatorio o se, comunque, destinati ad essere trasmessi in modo formale ai destinatari.

Il documento in arrivo può essere acquisito dall’Ordine con varie modalità, in base alla tecnologia di trasporto utilizzata dal mittente. Soprattutto nella fase di migrazione verso l’adozione integrale delle tecnologie digitali da parte degli enti e dei soggetti con i quali l’Ordine intrattiene rapporti, il documento amministrativo continuerà ad essere ricevuto anche nella forma analogica.

Un documento informatico può essere ricevuto:

1. a mezzo posta elettronica certificata;
2. a mezzo posta elettronica convenzionale;
3. a mezzo fax;
4. su supporto rimovibile - quale, ad esempio, CD, DVD, pen-drive, hard disk - consegnato direttamente o inviato per posta convenzionale o corriere;
5. per mezzo di sistemi telematici.

Un documento analogico può essere ricevuto:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telefax o telegramma;
4. con consegna diretta da parte dell’interessato o consegnato tramite persona dallo stesso delegata.

#### **3.1. DOCUMENTO INFORMATICO RICEVUTO SU CASELLA PEC ISTITUZIONALE**

##### **3.1.1. Documento ricevuto di competenza dell’Ordine**

Il documento ricevuto tramite la casella istituzionale di PEC (*presidenza@pecodcec.roma.it*) è gestito dalla UO Segreteria di Presidenza che provvede sempre alla registrazione di protocollo, ovvero al completamento della registrazione di protocollo e all’assegnazione alla UO di competenza, indipendentemente dal contenuto della PEC.

Il personale addetto alla Segreteria di Presidenza accede, regolarmente ed almeno due volte al giorno, alla casella PEC istituzionale per verificare la ricezione di eventuali nuovi messaggi.

Contestualmente al processo di protocollazione, l’addetto verifica se il mittente è presente in anagrafe Ordine e, in caso contrario, procede al suo censimento.

In ogni caso se il mittente, pur essendo censito, non ha l’indirizzo PEC in anagrafe Ordine, l’addetto può censire l’indirizzo PEC istituzionale/aziendale/professionale/personale, risultante da pubblici elenchi, avendo cura di evitare ogni forma di duplicazione del soggetto.



I pubblici elenchi sono il registro delle imprese, gli albi e gli elenchi istituiti con leggi dello Stato consultabili tramite il servizio INI-PEC, Indice nazionale indirizzi PEC (<http://www.inipec.gov.it/>), istituito dal Ministero dello Sviluppo Economico. Tra i pubblici elenchi rientrano, altresì, l'Indice delle Pubbliche Amministrazioni – iPA (<http://www.indicepa.gov.it/>), e l'Indirizzario dei Cittadini per la PA all'interno del servizio PostaCertificat@ (<http://www.postacertificata.gov.it/>), gestiti entrambi dall'Agenzia per l'Italia Digitale.

### **3.1.2. Documento ricevuto non di competenza dell'Ordine**

L'operatore, in caso di manifesto errore di invio, trasmette al mittente tramite la casella PEC istituzionale un messaggio recante la dicitura *“Comunicazione pervenuta per errore - non di competenza dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma”*, riportando l'oggetto del messaggio ricevuto.

## **3.2. DOCUMENTO INFORMATICO RICEVUTO SULLE ALTRE CASELLE PEC OPERATIVE E FUNZIONALI**

### **3.2.1. Documento di competenza della UO**

Ogni Ufficio UO dispone di una casella di PEC, gestita dai dipendenti dell'ufficio che provvedono a completare le operazioni di protocollazione e assegnazione all'interno di iShareDoc.

Il documento ricevuto nella casella PEC (funzionale) è gestito e protocollato all'interno di iShareDoc da parte degli addetti alla gestione della casella PEC individuati dalla Direzione al momento della attivazione della casella.

Il personale addetto agli uffici o alle caselle PEC funzionali accede regolarmente ed almeno due volte al giorno verifica la ricezione di eventuali nuovi messaggi ricevuti tramite PEC.

### **3.2.2. Documento di competenza non esclusiva della UO**

Il personale degli uffici procede all'assegnazione anche alle altre UO eventualmente interessate.

Se la corrispondenza è riservata, il RdU/RdUNC determina il livello di riservatezza e dispone il suo trattamento secondo la regolamentazione interna sulla riservatezza (cfr. A1 – Normativa di riferimento e bibliografia).

Qualora il documento sia indirizzato anche al Presidente o al Direttore, il personale della UO procede all'assegnazione anche alla Segreteria di Presidenza o alla Direzione.

### **3.2.3. Documento non di competenza della UO**

Il personale della UO riassegna immediatamente la corrispondenza ad altra UO, ove risulti chiara la competenza di quest'ultima; in caso contrario provvede ad assegnarla alla Direzione indicando nelle annotazioni *“Alla Direzione per riassegnazione a UO di competenza”*.

## **3.3. DOCUMENTO INFORMATICO RICEVUTO A MEZZO FAX**

Il documento informatico ricevuto a mezzo fax-server sotto forma di documento elettronico è preso in carico dal Protocollo o dalla Segreteria di presidenza. Il Protocollo e la Segreteria di presidenza procedono all'estrazione del file, al suo inserimento in iShareDoc, alla protocollazione e all'assegnazione alla UO di competenza, indicando contestualmente nell'annotazione *“Documento ricevuto via fax”*. La segnatura di protocollo è riportata in automatico nella relativa scheda documentale.



### **3.4. DOCUMENTO INFORMATICO RICEVUTO SU CASELLA E-MAIL CONVENZIONALE**

Il documento ricevuto via e-mail nelle caselle dell'Ordine non certificate rilevante dal punto di vista amministrativo è trasformato, a cura del ricevente, in un documento formato PDF e inserito, classificato e fascicolato nel sistema iShareDoc, indicando i suoi eventuali allegati. Il documento è protocollato dal personale della UO ricevente.

#### **3.4.1. Documento ricevuto di competenza della UO**

Il personale addetto alle UO accede, regolarmente ed almeno due volte al giorno, alla casella e-mail per verificare la ricezione di eventuali nuovi documenti.

#### **3.4.3. Documento ricevuto di competenza non esclusiva della UO**

Il personale della UO ricevente procede alle operazioni di accettazione, protocollazione e assegnazione anche alle altre UO interessate.

Se il documento è riservato dispone il suo trattamento secondo la regolamentazione interna sulla riservatezza (cfr. A1 – Normativa di riferimento e bibliografia).

#### **3.4.4. Documento ricevuto non di competenza della UO**

Il personale della UO ricevente può riassegnare immediatamente la corrispondenza ad altra UO, ove risulti chiara la competenza di quest'ultima; in caso contrario tale corrispondenza è assegnata alla Direzione, indicando nelle annotazioni "Alla Direzione per riassegnazione a UO di competenza".

### **3.5. DOCUMENTO INFORMATICO RICEVUTO SU SUPPORTO RIMUOVIBILE**

Nei casi in cui, in allegato ad un documento analogico, siano inviati documenti digitali su supporti rimovibili, l'UO ricevente procede alla protocollazione del documento analogico nonché allo scarico dei documenti elettronici dal supporto e alla loro acquisizione come allegati: in presenza di specifiche e congiunturali criticità - previo accordo con le UO di competenza - le predette attività di scarico ed acquisizione dei documenti elettronici possono essere differite secondo la tempistica di volta in volta concordata.

### **3.6. DOCUMENTO INFORMATICO RICEVUTO TRAMITE SISTEMI TELEMATICI - SPORTELLO DIGITALE**

Lo "Sportello Digitale" dell'Ordine consente a tutti gli Iscritti all'Albo, all'Elenco Speciale e al Registro del Tirocinio di presentare agli uffici dell'Ordine istanze e autocertificazioni in via telematica ai sensi degli artt. 64 e 65 del Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82). Lo Sportello è attivo senza soluzione di continuità in termini di orario e prevede il rilascio progressivo in modalità on-line dei servizi disponibili agli Iscritti.

Lo Sportello è accessibile dalle sezioni del sito web dell'Ordine relative ai servizi per cui è stata attivata la modalità di richiesta on-line.

Al primo accesso allo Sportello, previa identificazione dell'interessato, viene rilasciata la firma elettronica che consentirà all'Iscritto di presentare istanze in via telematica all'Ordine (la firma elettronica è valida solo per operare con l'Ordine di Roma).



Lo sportello, attraverso un sistema di web service, è integrato nel sistema iShareDoc che automaticamente protocolla, assegna con notifica i documenti alla UO di competenza e, laddove possibile, fascicola il documento.

### **3.7. DOCUMENTO ANALOGICO RICEVUTO PRESSO IL PROTOCOLLO E LE SEGRETERIE**

L'accettazione della corrispondenza, consegnata a mano oppure trasmessa mediante raccomandata, posta semplice, corriere o telegramma, avviene, di norma, negli orari di apertura al pubblico degli uffici.

Possono ricevere i documenti in arrivo:

- lo Sportello aperto al pubblico;
- l'ufficio Protocollo;
- la Segreteria del Consiglio di Disciplina;
- la Segreteria di Presidenza.

In caso di necessità, su espressa richiesta della Direzione o dei Consiglieri dell'Ordine, il personale abilitato procede all'accettazione di specifici documenti anche al di fuori dell'orario di apertura al pubblico degli uffici.

### **3.8. ACCETTAZIONE DI DOCUMENTO ANALOGICO**

Il personale addetto allo Sportello, al Protocollo e alle Segreterie tratta la corrispondenza secondo i seguenti tre raggruppamenti:

<b>Tipologia di corrispondenza</b>	<b>Trattamento</b>
Corrispondenza indirizzata direttamente a Presidente, Consiglieri, Direttore	<ul style="list-style-type: none"><li>- la busta non è aperta</li><li>- è trasmessa alle Segreterie competenti</li></ul>
Corrispondenza riportante la dicitura "Riservato" o "Personale" o corrispondenza valutata come tale	<ul style="list-style-type: none"><li>- la busta non è aperta</li><li>- è trasmessa all'interessato</li></ul>
Corrispondenza che non rientra nei due casi precedenti	<ul style="list-style-type: none"><li>- la busta è aperta</li><li>- si procede all'assegnazione</li></ul>

La corrispondenza indirizzata direttamente a Presidente, Consiglieri, Direttore ovvero classificata come "riservata" o "personale" è fatta pervenire direttamente all'interessato (o alla Segreteria competente) che, ove lo ritenga, trasmette il documento alla UO competente affinché proceda alla protocollazione e all'assegnazione del documento medesimo.

Il personale addetto allo Sportello, al Protocollo o alle Segreterie procede all'accettazione svolgendo le seguenti operazioni:

<b>Mezzo di ricezione</b>	<b>Verifiche</b>	<b>Operazioni</b>
Consegna a mano	Verifica della completezza della documentazione (es. corretto)	Emissione Ricevuta





	destinatario, presenza sottoscrizione autografa).	
Raccomandata A/R	Verifica della completezza della documentazione (es. corretto destinatario, numero allegati ove presenti). Verifica delle distinte delle raccomandate	Apposizione Timbro “ricevuto” sulla cartolina e sull’ulteriore documentazione prevista dal vettore.
Raccomandata, lettera semplice		Accettazione o rinvio al mittente
Telegramma		Apposizione Timbro “ricevuto” sul registro previsto dal vettore.
Corriere		Apposizione Timbro “ricevuto” sul registro previsto dal vettore.

Esaurite le operazioni relative all’accettazione, il personale addetto procede alla scansione e alla verifica della rispondenza del documento digitalizzato (copia informatica del documento analogico) con l’originale cartaceo. Successivamente l’addetto procede con la protocollazione, la segnatura e l’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 equivalgono all’attestazione di conformità della copia dei documenti informatici all’originale.

### **3.9. ACCETTAZIONE DI DOCUMENTO ANALOGICO PRESSO LE UO**

#### **3.9.1. Documento analogico di competenza, anche non esclusiva, della UO**

Il personale procede direttamente alle operazioni di accettazione, protocollazione, segnatura di protocollo tramite apposizione della etichetta riportante il numero di protocollo, scansione e assegnazione anche alle altre UO interessate.

Nel caso in cui il documento sia ricevuto fuori orario, su espressa richiesta della Direzione o dei Consiglieri, il personale procede alle operazioni di accettazione, protocollazione, segnatura di protocollo tramite apposizione della etichetta riportante il numero di protocollo, scansione e assegnazione. Ove la competenza non sia esclusiva della UO, la stessa assegna il documento anche alle altre UO interessate.

Se il documento è riservato, si applicano le prescrizioni secondo la regolamentazione interna sulla riservatezza.





### **3.9.2. Documento analogico non di competenza della UO**

Tali documenti sono immediatamente trasmessi alla UO di competenza.

## **3.10. DOCUMENTI ANALOGICI CHE NECESSITANO DI TRATTAMENTO PARTICOLARE**

### **3.10.1. Documenti non scansionabili contestualmente alla ricezione**

Le tipologie documentali che rientrano in questa sezione sono i documenti con numero di pagine superiore a 300 ovvero i documenti rilegati in formato non ricostruibile dopo la rimozione delle rilegature tipografiche, ovvero altri documenti che comportano particolari problemi di scansione (ad es. i documenti con timbri apposti sulle rilegature tra le pagine).

#### *Modalità di trattamento*

L'addetto procede all'accettazione, alla protocollazione e all'assegnazione senza la scansione. Il documento cartaceo è assegnato alla UO master destinataria e alle eventuali altre UO coassegnatarie e nella relativa scheda documentale viene annotato il fatto che il documento è stato assegnato in originale cartaceo alla UO master.

Qualora il documento sia munito di una lettera accompagnatoria, il ricevente la scansiona e la invia alle UO assegnatarie in formato digitale tramite iShareDoc.

La Segreteria della UO master procede alla sottoassegnazione del documento cartaceo al RdP. Questi provvede all'apertura di un fascicolo cartaceo con lo stesso numero di quello elettronico (ove già esistente, in caso contrario provvede alla sua creazione) e alla sua conservazione fino al momento del versamento nell'archivio.

Qualora si rilevi la necessità della disponibilità del documento anche da parte di altre UO, le segreterie interessate concordano, di volta in volta, con il Protocollo i tempi di scansione del documento.

### **3.10.2. Documenti riservati o personali**

Sono considerati tali i documenti in busta chiusa recanti la dicitura riservato o personale e direttamente indirizzati a Presidente, Consiglieri, Direttore.

#### *Modalità di trattamento*

Il documento è accettato dallo Sportello, dal Protocollo o dalla Segreteria e trasmesso in busta chiusa al destinatario. Ove il destinatario (Presidente, Consiglieri, Direttore), presa visione del documento, lo ritenga, dispone per l'invio del documento originale e della relativa busta all'UO competente, eventualmente con le indicazioni relative al livello di riservatezza. La UO procede con le normali operazioni di acquisizione del documento cartaceo, tenendo presente il livello di riservatezza indicato.

### **3.10.3. Atti giudiziari notificati**

#### *Modalità di trattamento*

Gli originali cartacei sono trasmessi alla UO competente; per assicurare la completezza del fascicolo cartaceo ed elettronico, la UO competente provvede all'acquisizione digitale e all'assegnazione alla UO competente. Il responsabile del procedimento avrà cura di conservare i documenti originali fino al momento dell'archiviazione.



#### **3.10.4. Atti relativi a procedure di gara o ad offerte**

##### *Modalità di trattamento*

Le relative buste non vengono aperte; il Protocollo appone sulla busta la data e l'ora di arrivo, protocolla con la segnatura applicata sull'esterno del plico e consegna la busta chiusa all'Ufficio competente. La scansione dei documenti di offerta e delle buste, l'inserimento nel sistema iShareDoc, la classificazione e la fascicolazione è eseguita dall'Ufficio competente a seguito della apertura del plico secondo quanto previsto nel bando di gara.

#### **3.10.5. Documenti non attinenti alle attività dell'Ordine**

##### *Modalità di trattamento*

- Se la busta non viene aperta, si restituisce alla posta;
- Se la busta viene aperta per errore, il documento non è protocollato e gli addetti al protocollo richiudono la busta apponendovi il timbro dell'Ordine, con data e firma e la dicitura "*Restituita perché pervenuta per errore*".

#### **3.11. REGISTRAZIONE DI PROTOCOLLO E RELATIVA SEGNATURA**

Superati i controlli precedenti, i documenti, digitali o analogici, sono protocollati e "segnati" nel protocollo generale in iShareDoc.

#### **3.12. SMISTAMENTO E ASSEGNAZIONE ALLE UOP**

Lo smistamento dei documenti all'interno dell'Ordine avviene, di norma, attraverso il sistema iShareDoc, mediante assegnazione all'UO Master e ad eventuali UO cointeressate .

Contestualmente l'assegnazione avviene con visibilità per competenza alle UO master e delle altre UO assegnatarie e con eventuale visibilità per copia conoscenza alla Direzione.

L'assegnazione avviene automaticamente con notifica alle UO assegnatarie.

Il documento è assegnato direttamente a una singola o a più UO sulla base dei seguenti elementi:

- a) il documento riporta il numero di protocollo di una richiesta formulata da una o più UO;
- b) il contenuto, la natura e i riferimenti normativi del documento;
- c) la qualifica del mittente e la qualifica del soggetto;
- d) il documento riporta il numero di fascicolo di riferimento.

Qualora la UO master o la UO cointeressata ritenga che il documento trasmessole debba essere conosciuto o trattato da altra UO, provvede all'operazione di smistamento sopra descritta.

La trasmissione di documenti tra Uffici avviene esclusivamente attraverso l'operazione di assegnazione di documenti firmati e protocollati, sulla cui scheda documentale è possibile aggiungere annotazioni relative al documento stesso.

L'assegnazione a Presidente e ai Consiglieri avviene attraverso la Segreteria di presidenza:

- nei casi in cui la corrispondenza è ad essi direttamente indirizzata;
- nei casi in cui la particolarità dei contenuti e la specificità dei mittenti rendano evidente l'opportunità della immediata conoscenza da parte degli organi di vertice, previa eventuale consultazione degli uffici interessati;
- a seguito di specifiche indicazioni ricevute.

Nel caso in cui sia necessario trasmettere documenti cartacei alle UO, oltre ad aggiornare le annotazioni sulla relativa scheda documentale, gli addetti alla protocollazione li consegnano al



personale delle UO in relazione al segnalato carattere di urgenza o di rilevanza dei documenti stessi.

La circolazione dei documenti avviene nel rispetto delle disposizioni che regolano la diffusione della documentazione riservata, in funzione del livello di riservatezza di ciascuno di essi.

### **3.13. CLASSIFICAZIONE E FASCICOLAZIONE**

Il dipendente che protocolla il documento provvede a classificarlo secondo il Titolario dell'Ordine (cfr. Allegato 2 – Titolario di Classificazione) e a fascicolarlo secondo i principi e i criteri indicati nel capitolo 7 ed in base al Piano di Fascicolazione (Allegato 3 – Piano di Classificazione e Fascicolazione). Il dipendente al quale è assegnato il documento potrà modificare la classificazione e la fascicolazione, della quale il sistema i.ShareDoc manterrà traccia.

## **4. FLUSSI DI LAVORAZIONE DEI DOCUMENTI IN PARTENZA E A RILEVANZA INTERNA**

Di seguito sono descritti i flussi di lavorazione dei documenti inviati dall'Ordine, all'esterno o all'interno se di preminente carattere giuridico-probatorio o in modo formale.

Le fasi di lavorazione sono:

- predisposizione;
- approvazione;
- registrazione di protocollo e relativa segnatura del documento;
- invio.

I documenti interni sono di tipo informatico o analogico e sono trasmessi in via telematica attraverso le funzionalità di iShareDoc o le caselle e-mail PEC o convenzionali in dotazione alle UO. Il sistema iShareDoc è utilizzato per lo scambio di corrispondenza interna, sia formale che informale.

I documenti archiviati prima dell'avvio del processo di dematerializzazione (1° luglio 2015) sono consultabili avvalendosi dei precedenti sistemi documentali.

### **4.1. PREDISPOSIZIONE DEL DOCUMENTO IN PARTENZA E DEL DOCUMENTO INTERNO**

La fase di predisposizione di un documento ha avvio con la creazione del documento e si conclude con il consolidamento dello stesso in formato PDF o cartaceo.

È obbligatorio - prima di concludere la fase di predisposizione - classificare, fascicolare e individuare il livello di riservatezza del documento, oltre all'impostazione dei metadati obbligatori della scheda documentale.

Se la comunicazione avviene tramite PEC, la dimensione dei documenti allegati nella scheda documentale non deve superare complessivamente i limiti previsti dalla normativa vigente, altrimenti l'invio della PEC non va a buon fine.

Al termine il documento è "consolidato", ovvero trasformato nel formato PDF, rendendolo altresì immodificabile, e assegnato ai responsabili per il visto elettronico e/o la firma digitale in caso di documento analogico lo stesso è stampato per l'apposizione della firma autografa e successivamente acquisito in formato PDF nel sistema di protocollo.



#### **4.2. APPROVAZIONE**

Sono abilitati all'approvazione tramite firma digitale o autografa dei documenti, in funzione del tipo di documento:

- il Presidente;
- il Direttore;
- i Consiglieri;
- altri soggetti specificamente ed espressamente individuati.

Sono abilitati anche i relativi sostituti.

L'estensore assegna il documento ai firmatari. Al termine della raccolta delle firme l'estensore procede alla protocollazione e all'invio al destinatario.

#### **4.3. REGISTRAZIONE DI PROTOCOLLO E RELATIVA SEGNAZIONE**

La protocollazione di un documento in partenza è, di norma, eseguita dal personale della UO che prodotto il documento; tale funzione può essere svolta anche da altri addetti previa abilitazione autorizzata dal RGD o da un suo delegato, secondo gli standard e le modalità dettagliate nel capitolo 5.

#### **4.4. INVIO DEL DOCUMENTO**

Il canale preferenziale del documento in partenza è la PEC. Prima di avviare il processo di protocollazione, il personale addetto verifica se il destinatario dispone di indirizzo PEC nella rubrica del sistema iShareDoc. In caso contrario, può censire l'indirizzo PEC istituzionale/aziendale del destinatario - risultante da pubblici elenchi - nell'Anagrafe dell'Ordine, avendo cura di evitare la duplicazione del soggetto.

Gli abilitati attivano il processo di protocollazione e provvedono all'invio della PEC ai destinatari esterni qualora si disponga dell'indirizzo PEC.

La ricevuta di consegna della PEC è gestita dal sistema di invio della posta elettronica. In caso di mancata consegna è possibile reiterare l'invio della PEC attraverso un'apposita funzione disponibile nel medesimo sistema. L'invio all'esterno di un documento tramite PEC – corroborato dalla ricevuta di consegna da parte del destinatario - esclude la necessità di trasmettere il medesimo documento anche attraverso altri canali di trasmissione.

Se la dimensione complessiva dei documenti da inviare tramite PEC supera i limiti previsti dalla normativa, la trasmissione non è effettuata e il sistema di invio della PEC invia un messaggio all'addetto che dovrà dare immediato avvio alle successive operazioni di invio.

Qualora l'indirizzo PEC del destinatario non sia presente nella rubrica del sistema iShareDoc, oppure vi sia l'esigenza di inviare il documento ad un indirizzo PEC (c.d. PEC operativa) diverso rispetto a quello aziendale/istituzionale presente in Anagrafica, occorre aggiungere un "Nuovo indirizzo" (c.d. estemporaneo) nella scheda documentale. Tale indirizzo estemporaneo sarà esclusivamente utilizzato per la trasmissione della specifica scheda documentale e riportato nel campo "Destinatario" della scheda; al fine di evitare duplicazioni, non verrà trasferito nell'anagrafe dell'Ordine e, pertanto, per essere riutilizzato dovrà essere digitato *ex novo* ovvero dovrà essere duplicata la corrispondente scheda di predisposizione.

Nel caso in cui il destinatario non sia provvisto di PEC, l'invio avviene con le altre modalità disponibili e conformi alla natura dell'atto.



## **4.5. MATERIALIZZAZIONE DEL DOCUMENTO INFORMATICO**

### **4.5.1. Spedizione tramite posta**

Nel caso di invio tramite posta, l'addetto alla protocollazione rileva l'esatta modalità dalla rubrica del sistema iShareDoc e provvede alla stampa del documento. Qualora il documento vada anticipato via fax, il mittente avrà cura di indicarlo nelle Annotazioni.

L'addetto procede alla stampa e all'attestazione di conformità utilizzando l'apposita funzionalità di stampa. Per default la stampa avviene su carta intestata in bianco e nero. La stampa avviene su carta intestata nei casi previsti dalla normativa interna.

Nel caso in cui gli allegati superino cinquanta pagine sono trasferiti su un supporto esterno non riscrivibile (CD/DVD), da spedire unitamente al documento materializzato e ne è data evidenza nelle Annotazioni.

Successivamente il documento è imbustato e affrancato; è predisposta la cartolina di avviso di ricevimento nel caso di utilizzo del vettore raccomandata A/R:, sulla quale sono indicati il nome del destinatario, il relativo indirizzo, la sigla della UO mittente ed il numero di protocollo.

È, quindi, redatta una distinta dei documenti da inviare che riporta i seguenti dati principali:

- numero di raccomandata;
- destinatario;
- città di destinazione;
- numero di protocollo.

È, altresì, predisposta una nota riepilogativa riportante il numero dei plichi inviati e il costo totale della spedizione giornaliera.

Il personale addetto alla consegna della corrispondenza all'ufficio postale di riferimento effettua il ritiro dei plichi e della relativa documentazione di accompagnamento.

Completate le conseguenti operazioni di consegna, il medesimo personale archivia la distinta di avvenuta spedizione dei plichi presso il Protocollo.

Al momento della restituzione della cartolina di avviso di ricevimento da parte del sistema postale, il Protocollo provvede al suo smistamento presso le UO destinatarie, individuabili tramite la sigla dell'ufficio mittente apposta dall'addetto sulla cartolina prima dell'imbustamento del documento.

Le UO, ricevuta la cartolina, provvedono alla scansione della stessa e la allegano alla relativa scheda documentale.

### **4.5.2. Spedizione a mezzo fax**

In caso di invio tramite fax, l'addetto all'invio rileva il fatto dalla rubrica del sistema iShareDoc. L'istruttore avrà cura di allegare alla scheda documentale, oltre al documento da inviare, anche il file contenente la cover prevista adeguatamente compilata. L'addetto all'invio trasferisce tali file nel fax-server e procede, quindi, alla trasmissione via fax, compiuta la quale inserisce un'annotazione nella scheda documentale, riportante l'ora e l'esito della trasmissione. Il report di trasmissione del fax viene inserito in allegato alla scheda.

### **4.5.3. Consegna a mano**

Nel caso in cui sia necessario procedere alla consegna a mano, gli addetti alla UO competente materializzano il documento, ne attestano la conformità e procedono alle successive operazioni di consegna a mano al destinatario.



Qualora si renda necessario attestarne la ricevuta/accettazione da parte del destinatario, lo stesso riporta un'annotazione con la dicitura "Visto per ricevuta".

## **5. PRODUZIONE DEL PROTOCOLLO INFORMATICO**

Di seguito si illustrano le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

L'attività di protocollazione è svolta, di norma, dal personale delle UO e del Protocollo.

### **5.1. UNICITÀ DEL PROTOCOLLO**

Nell'ambito dell'Ordine il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica, indipendentemente dal modello organizzativo adottato.

Il Registro informatico ufficiale di protocollo è denominato in iShareDoc "Protocollo Ufficiale". La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. Il numero di protocollo è costituito da almeno sette cifre numeriche nell'anno.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Ne consegue che:

- non è consentita la protocollazione di un documento già protocollato (In caso di ricezione multipla dello stesso documento, si inserisce un'annotazione nella scheda documentale del documento protocollato: "Documento pervenuto in copia multipla" allegando tutte le copie);
- non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro;
- non è, infine, consentita la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici. Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

### **5.2. REGISTRO GIORNALIERO DI PROTOCOLLO**

Il RGD, ovvero suo delegato, provvede tramite il sistema alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno: numero e data di protocollo; stato (inserito, annullato); mittente o destinatario; oggetto; eventuale riferimento esterno.

Il registro giornaliero di protocollo è firmato digitalmente dal delegato e conservato, garantendone l'immodificabilità del contenuto.

I principali metadati del registro giornaliero di protocollo sono riportati nella tabella seguente

<b>Nome dato</b>	<b>Descrizione</b>	<b>Tipo</b>	<b>Modificabile</b>	<b>Obbligatori o</b>
<b>Archivio</b>	Registro giornaliero	File	No	Sì



<b>Tipo Documento</b>	Scheda RegISTRAZIONI	Testo	No	Sì
<b>Data Registrazione</b>	Data assegnata in automatico al momento della generazione del registro giornaliero di protocollo	Data	Automatico	Sì
<b>Nome File</b>	Descrizione assegnata in automatico dal sistema al momento della generazione del registro giornaliero	Testo	No	Sì

### 5.3. REGISTRAZIONE DI PROTOCOLLO

Di seguito sono illustrate le regole “comuni” di registrazione del protocollo valide per tutti i tipi di documenti trattati dall’Ordine (ricevuti, trasmessi, interni formali, informatici e analogici).

Su ogni documento ricevuto o spedito dall’Ordine è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un’unica operazione, senza possibilità per l’operatore di inserire le informazioni in più fasi successive.

La protocollazione avviene di norma entro la giornata di accettazione. Eventuali rilevanti differimenti di data devono essere motivatamente indicati nel campo “Annotazioni” della scheda documentale del “Protocollo Ufficiale”.

Ove siano presenti sufficienti elementi, l’addetto alla protocollazione individua il titolo e la classe del documento e li inserisce negli appositi campi.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente o il destinatario del documento, registrato in forma non modificabile, salvi i casi previsti dalla normativa;
- l’oggetto del documento, registrato in forma non modificabile, salvi i casi previsti dalla normativa.

In via eccezionale, è prevista la modifica parziale dell’oggetto del protocollo in ingresso le cui modifiche sono tracciate e rese visibili.

Le registrazioni di protocollo, in coerenza con la normativa vigente, prevedono elementi informativi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

In iShareDoc i dati della registrazione di protocollo e i relativi metadati sono suddivisi tra Protocollo in ingresso e Protocollo in uscita.





### Protocollo in ingresso

<b>Nome dato</b>	<b>Descrizione</b>	<b>Tipo</b>	<b>Modificabile</b>	<b>Obbligatorio</b>
<b>HASH</b>	Impronta del documento	Testo	Automatico	Sì
<b>Progressivo</b>	Numero identificativo assegnato in automatico al documento	Numerico	Automatico	Sì
<b>Data Registrazione</b>	Data assegnata in automatico al momento della generazione del registro giornaliero di protocollo	Data	Automatico	Sì
<b>Oggetto</b>	Contenuto del documento	Testo	Sì	Sì
<b>Mittente</b>	Soggetto da cui proviene il documento	Testo	Sì	Sì

### Protocollo in uscita

<b>Nome dato</b>	<b>Descrizione</b>	<b>Tipo</b>	<b>Modificabile</b>	<b>Obbligatorio</b>
<b>HASH</b>	Impronta del documento	Testo	Automatico	Sì
<b>Progressivo</b>	Numero identificativo assegnato in automatico al documento	Numerico	Automatico	Sì
<b>Data Registrazione</b>	Data assegnata in automatico al momento della	Data	Automatico	Sì





	generazione del registro giornaliero di protocollo			
<b>Oggetto</b>	Contenuto del documento	Testo	Sì	Sì
<b>Destinatari</b>	Soggetto a cui è trasmesso il documento	Testo	Sì	Sì

Il RGD, al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può disporre la modifica e l'integrazione degli elementi non obbligatori del protocollo.

La registrazione degli elementi facoltativi del protocollo può essere modificata, integrata e cancellata dal RGD, o suoi delegati, in base alle effettive esigenze delle UO o degli UOP.

I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

#### **5.3.1. Documenti informatici**

I documenti informatici sono ricevuti e trasmessi in modo formale sulla e dalla casella di posta elettronica certificata istituzionale dell'Ordine.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la firma.

Nel caso di documenti informatici in partenza, l'utente esegue anche la verifica della presenza della firma o delle firme necessarie per dare giuridica rilevanza ai documenti stessi. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

I documenti informatici sono memorizzati nel sistema al termine delle operazioni di registrazione e segnatura di protocollo.

#### **5.3.2. Documenti analogici e supporti rimovibili**

La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato, viene sempre eseguita.

Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato i controlli formali sopra richiamati.

#### **5.4. LIVELLO DI RISERVATEZZA**

Qualora l'addetto alla protocollazione valuti il documento come non riservato, non è necessario impostare alcun livello di riservatezza.

Qualora, invece, il documento sia valutato di natura riservata, l'addetto alla protocollazione gli assegna la conseguente classificazione e procede come indicato nella regolamentazione interna sul trattamento dei documenti contenenti dati sensibili (DPS).

Al momento il sistema prevede dunque due livelli di riservatezza così definiti:



- livello non riservato: a diffusione interna (relativo a documenti esportabili su internet e a documenti esportabili su intranet dell'Ordine);
- livello riservato: a consultazione limitata (relativo a documenti consultabili solo dalla UO di competenza).

### **5.5. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI**

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

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

Le informazioni sono abbinate in maniera univoca a ciascun documento protocollato e memorizzate nel Registro di "Protocollo Ufficiale". Nel sistema iShareDoc a ciascuna registrazione di protocollo è associato il corrispondente documento elettronico con eventuali relativi allegati, attraverso la scheda documentale che ne integra anche i relativi metadati.

#### **5.5.1. Documenti informatici**

I dati della segnatura di protocollo di un documento informatico sono:

- identificativo dell'Ordine;
- data e numero di protocollo del documento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

#### **5.5.2. Documenti analogici**

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un'etichetta grafica adesiva sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- identificativo dell'Ordine;
- entrata/uscita;
- data e numero di protocollo del documento.

Facoltativamente possono essere riportate anche le seguenti informazioni:

- il codice identificativo dell'UO a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo;
- ogni altra informazione utile o necessaria, se già disponibile al momento della registrazione di protocollo.

Dopo la registrazione di protocollo di un documento analogico, l'operatore:

- stampa l'etichetta adesiva di segnatura, che incolla sul documento;
- procede alla scansione del documento tramite scanner e ne verifica la rispondenza all'originale per la contestuale attestazione di conformità. Il sistema associa il documento alla scheda documentale di protocollo generata nella fase di registrazione;
- assegna il documento alle strutture competenti;



- archivia, possibilmente entro la giornata di protocollazione, l'originale cartaceo del documento presso l'archivio della UO di pertinenza in ordine di numero di protocollo.

La segnatura è realizzata con una etichetta autoadesiva corredata di codice a barre (cfr. A8 – Loghi, timbri, etichette Ordine), che viene apposta alla prima pagina del documento originale.

In caso di indisponibilità o malfunzionamento del sistema di etichettatura, l'operazione di segnatura sul documento analogico con data e numero di protocollo è effettuata dall'operatore direttamente sul documento.

L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguita solo dopo l'operazione di segnatura, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Per i documenti in partenza materializzati, in particolare, la segnatura viene apposta con la stampa del numero e della data di protocollo, generate dal sistema informatico.

#### **5.6. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO**

La modifica di un campo obbligatorio della registrazione di protocollo, generata automaticamente dal sistema, comporta l'obbligo di annullare l'intera registrazione di protocollo.

La funzione di annullamento delle registrazioni di protocollo è accessibile solo al RGD, ai suoi delegati mediante apposita richiesta di annullamento e previa valutazione della stessa. L'operazione è, ad ogni modo, registrata nella scheda documentale e segnalata dal sistema al RGD, con un messaggio in iShareDoc in cui è indicato il protocollo annullato, l'utente, la data e l'ora dell'operazione.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo.

Il RGD, o suoi delegati, ha la possibilità di ripristinare un protocollo annullato in caso di errore nella precedente operazione di annullamento o per specifiche esigenze amministrative.

L'annullamento anche di un solo campo delle altre informazioni registrate in forma immutabile, non generate automaticamente dal sistema, per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.

#### **5.7. PROTOCOLLO DI EMERGENZA**

Nei casi di temporanea indisponibilità previsti dalla normativa vigente, il servizio di Protocollo può assegnare alle UO che ne facciano richiesta numeri di protocollo di "emergenza", tratti da una sequenza del tutto distinta da quella del "protocollo ufficiale", in base ad apposito registro.

Il protocollo di emergenza è avviato, previa autorizzazione del RGD o suoi delegati, qualora per cause tecniche non sia possibile utilizzare la procedura informatica iShareDoc per un periodo di tempo rilevante ai fini della gestione dei procedimenti.

Una volta ripristinate le normali funzionalità del sistema, il servizio di Protocollo, ovvero le UO, provvedono a registrare in iShareDoc, in corrispondenza dei "protocolli ufficiali", i relativi protocolli di "emergenza".

I numeri di protocollo di "emergenza" richiesti e non utilizzati sono eliminati dal registro.



Il registro di emergenza è gestito da un sistema dedicato, separato dalla piattaforma iShareDoc e dislocato presso le strutture di Protocollo.

#### **5.8. DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E CASI PARTICOLARI DI REGISTRAZIONE**

La casistica dei documenti esclusi dalla protocollazione e dei casi particolari di registrazione di protocollo sono descritti in A7 – Elenco dei documenti esclusi dalla registrazione di protocollo.

#### **5.9. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO TRAMITE ISHAREDOC**

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate mediante il sistema iShareDoc.

Il sistema di sicurezza adottato dall'Ordine provvede alla protezione di tali informazioni sulla base dell'architettura del sistema informativo, dei controlli d'accesso e dei livelli di autorizzazione previsti.

#### **5.10. CARATTERISTICHE DEL REGISTRO INFORMATICO DI PROTOCOLLO**

##### **5.10.1. Riferimento temporale del protocollo**

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, la funzionalità di protocollo informatico è realizzata dal sistema iShareDoc attraverso l'apposizione di un riferimento temporale, come previsto dalla normativa vigente. Il sistema informatico gestisce la precisione del riferimento temporale con l'acquisizione del tempo del server di sistema.

##### **5.10.2. Registro informatico di protocollo**

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale dell'Ordine si provvede, in fase di chiusura giornaliera dell'attività di protocollo, ad effettuare le seguenti operazioni:

- estrazione delle registrazioni del giorno precedente dal file del registro generale di protocollo;
- archiviazione del file del registro con la firma digitale sul sistema e il relativo riferimento temporale.

L'addetto alla conservazione è delegato ad eseguire l'operazione di riversamento dei file nel sistema di conservazione (vd capitolo 8).

L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo.

È inoltre disponibile, all'occorrenza, per i gestori del sistema una funzione applicativa di "stampa registro di protocollo" per l'eventuale salvataggio esterno dei dati di registro.

##### **5.10.3. Tenuta del registro giornaliero di protocollo**

È compito del responsabile della conservazione dei documenti, o suoi delegati, provvedere alla verifica del registro giornaliero di protocollo e alle operazioni relative al trasferimento del registro nel sistema di conservazione.

Il registro giornaliero di protocollo generato dal sistema è gestito e conservato dal RGD, o suoi delegati con le modalità indicate nel presente manuale.



### **5.11. DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO**

La descrizione funzionale ed operativa del sistema iShareDoc, incluso il sistema di protocollo informatico e di gestione dei flussi documentali, è parte del presente manuale (Allegato 1 – iShareDoc 3.0 Guida utente).

## **6. SISTEMA DI GESTIONE ARCHIVISTICA**

### **6.1. GENERALITÀ**

Di seguito si richiamano i principi e si descrivono gli strumenti archivistici dell'Ordine per la formazione e gestione dell'archivio corrente, con particolare riferimento al titolario, ai fascicoli e alle modalità di loro impiego.

### **6.2. MISURE DI TUTELA E VALORIZZAZIONE DELL'ARCHIVIO DELL'ORDINE**

L'Ordine, in quanto ente con personalità giuridica di diritto pubblico munito di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, non è soggetto alle disposizioni in vigore per le amministrazioni statali per quanto attiene alla tenuta degli archivi e allo scarto.

La documentazione prodotta dall'Ordine non è, quindi, sottoposta al vaglio delle Commissioni di sorveglianza e scarto, ma è tutelata dalla Soprintendenza archivistica per territorio che vigila, quale Organo di controllo, anche sull'osservanza dell'obbligo dell'Ordine di ordinare e inventariare i propri archivi storici rendendoli accessibili alla consultazione.

L'archivio e i singoli documenti dell'Ordine sono, in generale, beni a carattere culturale. I documenti trattati (analogici ed informatici, ricevuti, spediti e interni formali) sono da ritenersi inalienabili ed inseriti nell'archivio dell'Ordine, di norma mediante l'attribuzione di un numero di protocollo e/o di un indice di classificazione.

L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità. Il trasferimento ad altri soggetti esterni di complessi organici di documentazione nonché lo scarto dei documenti degli archivi dell'Ordine sono subordinati all'autorizzazione della Soprintendenza archivistica.

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

### **6.3. TITOLARIO DELL'ORDINE**

Il Titolario è il sistema precostituito di partizioni astratte, gerarchicamente ordinate (dal generale al particolare), fissate sulla base dell'analisi delle funzioni e delle attività dell'Ordine, al quale deve ricondursi la molteplicità dei documenti prodotti, per organizzarne l'ordinata sedimentazione.

Il Titolario dell'Ordine si articola in titoli e classi. Il titolo (o voce di 1° livello) individua le funzioni primarie e di organizzazione (macrofunzioni); le classi (o voci di 2° livello) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nel Titolario di Classificazione (Allegato 2).



Per ciascun livello è previsto il relativo “Indice di classificazione”, cioè il valore numerico che lo identifica in maniera univoca. Il Titolare dell’Ordine adotta una numerazione mediante cifre indoarabiche separate dal punto.

Titoli e classi sono nel numero prestabilito dal Titolare e non sono modificabili né nel numero né nell’oggetto, se non mediante espresso provvedimento emendativo.

Il Titolare è uno strumento suscettibile di aggiornamento: esso deve, infatti, sempre descrivere le funzioni e le competenze dell’Ordine, suscettibili di modifiche in forza di specifiche disposizioni normative.

L’approvazione e le modifiche del Titolare sono di competenza del Consiglio dell’Ordine.

#### **6.4. CLASSIFICAZIONE DEI DOCUMENTI**

La classificazione è l’operazione finalizzata all’organizzazione dei documenti, secondo un ordine logico, in relazione alle funzioni e alle competenze dell’Ordine; essa è obbligatoria per legge.

L’operazione di classificazione di un documento consiste in un processo di *reductio ad unum*, cioè a dire di riconduzione a unità logiche di una molteplicità di casistiche.

Anche in ragione di ciò, il titolare è uno strumento di gestione documentale onnicomprensivo, finalizzato a prevedere e organizzare quanto l’Ordine pone e porrà in essere sul piano documentale nell’ambito delle funzioni sue proprie.

Tutti i documenti ricevuti e prodotti dalle UO dell’Ordine indipendentemente dal supporto sul quale vengono formati, sono classificati in base al Titolare.

Mediante la classificazione si assegna al documento l’indice di classificazione costituito da titolo e classe.

L’Ordine prevede che l’operazione di classificazione possa essere svolta in momenti diversi: o già all’atto della protocollazione ovvero, dopo l’assegnazione, dall’incaricato della trattazione della pratica.

È posto in coda al titolare, conformemente alla prassi archivistica, il titolo “oggetti diversi”, che non prevede classi, dedicato al carteggio e, più in generale, alla documentazione non riconducibile ai titoli e alle classi previsti e riferentesi a funzioni e attività non rientranti tra le attribuzioni dell’Ordine alla data di approvazione del titolare.

Il suo impiego è, pertanto, da ritenersi eccezionale, mentre il suo significato non è da intendersi come sinonimo di documentazione “miscellanea” o “varia”.

Nel caso di classificazione del documento in questo titolo, quindi, l’utente è tenuto a contattare in particolare il delegato per la tenuta del protocollo e il delegato per la gestione documentale e gli archivi e definire congiuntamente la classificazione opportuna.

#### **6.5. FASCICOLAZIONE DEI DOCUMENTI**

Tutti i documenti registrati nel sistema informatico e classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli. La fascicolazione è obbligatoria per tutti i documenti, anche quelli non protocollati.

Ogni documento, dopo la sua classificazione, è inserito nel fascicolo di riferimento.

I documenti sono archiviati all’interno di ciascun fascicolo o, all’occorrenza, sottofascicolo secondo l’ordine cronologico di registrazione.



Il sistema iShareDoc consente la “**multifascicolazione**” dei documenti. Se un documento si riferisce a più procedimenti e attività, è possibile inserirlo in più fascicoli.

Questo tipo di funzione è particolarmente utile, fra l’altro, per la gestione di documentazione relativa a procedimenti 241, correlata logicamente e funzionalmente ed accessoria ad un altro procedimento amministrativo più “ampio”. In questi casi, il documento è inserito in più fascicoli: sia in quello del procedimento più ampio, sia in quello correlato. A tal riguardo si avrà cura di collegare i due fascicoli attraverso la funzione di sistema dedicata.

## **6.6. PIANO DI FASCICOLAZIONE**

La mappatura delle tipologie di fascicoli previste dall’Ordine, con indicazione delle relative denominazioni standard, al fine di facilitarne la creazione e la gestione da parte degli utenti abilitati, è indicata nel Piano di fascicolazione (Allegato 3 – Piano di Classificazione e Fascicolazione).

Il Piano di fascicolazione segue la struttura del Titolario ed è soggetto ad apposite procedure di aggiornamento e revisione, attraverso richieste formali e confronti con il RGD o il delegato per la gestione documentale e gli archivi al fine di favorire l’aggiornamento di uno strumento che è patrimonio informativo e gestionale dell’Ordine.

## **6.7. TIPOLOGIE E DURATA DEL FASCICOLO**

Il fascicolo è l’unità archivistica prevalente nell’archivio ed il vero e proprio “cuore” della sua organizzazione. Inteso come la raccolta ordinata, prevalentemente secondo una sequenza cronologica, di tutti i documenti (da e verso l’esterno, interni, protocollati e non protocollati, documenti di lavoro) relativi a una determinata pratica, il fascicolo riveste una centralità sotto molteplici profili: da quello giuridico a quello gestionale.

Per quanto attiene ai profili e alle finalità nonché al tipo di documentazione che raccoglie, nell’Ordine sono state previste quattro tipologie di fascicolo:

1. Fascicolo “Procedimento 241” e “Fascicolo istruttorio”
2. Fascicolo “Attività”
3. Fascicolo di “Iscritto Persona fisica o giuridica”
4. Fascicolo “Standard”

### **6.7.1. Fascicolo “Procedimento 241” e fascicolo “Istruttorio”**

Sono i fascicoli definiti (con terminologia archivistica) “per affare”: essi riguardano una competenza proceduralizzata o un’attività amministrativa omogenea, destinate a concludersi con un provvedimento finale ovvero con un documento che ne sancisce la chiusura. Sono, pertanto, i fascicoli che attengono principalmente, ma non solo, ai procedimenti amministrativi.

Nello specifico, il fascicolo “241” è un fascicolo che, ai sensi dell’art. 41 del CAD, raccoglie gli atti, i documenti e i dati del procedimento amministrativo cui si riferisce.

Tali fascicoli si aprono al livello più basso del titolare di classificazione; quindi, nell’ambito di una delle classi e comprendono i documenti, recanti in genere tutti la medesima classifica, prodotti da una o più UO per la trattazione dell’affare.





Il *fascicolo per affare* ha una data di apertura, una durata, che ovviamente può non coincidere con l'anno solare, e una data di chiusura: può, comunque, essere gestito anche su base annuale, in quanto viene "trasportato a nuovo anno" se non chiuso nell'anno di apertura.

Quali meri e puramente indicativi esempi di *fascicoli per affare* dell'Ordine:

- il fascicolo richiesta di iscrizione Albo;
- il fascicolo disciplinare.

### **6.7.2. Fascicolo di "attività"**

Indica un fascicolo relativo ad attività amministrativa semplice, non proceduralizzata, non discrezionale e ripetitiva, a cadenza predefinita, generalmente annuale, che si esaurisce in risposte obbligate o in meri adempimenti.

Il fascicolo per attività può comprendere documenti con destinatari e oggetti diversi, ma generalmente con identica classifica; se la massa documentale è eccessiva, può articolarsi in sottofascicoli secondo ulteriore articolazione temporale o di altro tipo come soggetti, materie etc.

Quali esempi:

- il fascicolo delle richieste di informazioni;
- il fascicolo relativo alla corrispondenza.

### **6.7.3. Fascicolo di "persona fisica o giuridica"**

Indica il fascicolo del personale oppure il fascicolo relativo ad una persona giuridica. Raccoglie tutti i documenti, anche con classifiche diverse, che si riferiscono ad un determinato soggetto.

Per quanto attiene al fascicolo del personale, cioè del dipendente, esso si configura concettualmente come un'aggregazione di documenti diversamente classificati: esso è propriamente un fascicolo multi-affare, multi-attività e multi-procedimentale. Non contiene tutti i documenti di un determinato affare, di un determinato procedimento amministrativo o di una determinata attività, ma solo quelli che servono a ricostruire gli eventi giuridici, organizzativi ed economici che riguardano una persona che intrattiene o ha intrattenuto un rapporto strutturato di lavoro con l'Ordine. Pertanto, esso serve, da un lato, a documentare la carriera di un lavoratore per gli aspetti giuslavoristici e, dall'altro, a determinare il trattamento giuridico-economico, pensionistico o di fine rapporto.

Com'è ovvio, quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte, e di tale caratteristica tiene conto il sistema di gestione documentale.

Questo tipo di fascicolo si può aprire a livello di titolo (ad esempio, per i dipendenti) e a livello di classe (plausibile secondo le esigenze organizzative dell'Ordine come, a esempio, il Fascicolo Iscritto).

Quanto osservato vale, con le differenze del caso, anche per il fascicolo per "soggetto giuridico" (ad es. STP iscritta nell'Albo), nel quale si andranno a raccogliere i documenti propri che attengono a quel determinato soggetto.

A tale proposito, per l'Ordine, è previsto l'utilizzo di fascicoli di tal tipo per la raccolta dei documenti connessi ad attività di "tenuta dell'Albo e del Registro del tirocinio".





#### **6.7.4. Fascicolo “standard”**

Accanto a tali tipologie principali va aggiunto il cosiddetto *fascicolo “standard” o di lavoro*, che raccoglie in prevalenza “documenti di lavoro” non necessariamente protocollati: è quello che il dipendente apre a proprio uso e consumo, ovvero per le esigenze gestionali della UO, vale a dire che egli impiega per ragioni connesse al lavoro e come supporto alle attività che svolge. La documentazione si sostanzia per lo più in copie di documenti, già presenti nei fascicoli archivistici, minute di documenti interni, bozze, etc., i cui originali esemplari definitivi sono conservati nell’archivio. Tale tipo di fascicolo, quindi, dovrà essere attentamente vagliato e selezionato una volta che il procedimento o le attività cui si riferisce siano conclusi, onde valutare adeguatamente l’opportunità di porlo in conservazione nella sua interezza ovvero solo per alcune sue parti ovvero ancora scartarlo del tutto.

#### **6.8. APERTURA DEL FASCICOLO**

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, il dipendente preposto provvede all’apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l’operazione di “apertura” che comprende la registrazione di alcune informazioni essenziali. Di seguito si riportano i metadati del fascicolo suddivisi per area di riferimento ai relativi standard.

#### **6.9. OGGETTO DEL FASCICOLO**

L’oggetto del fascicolo è una stringa di testo che descrive compiutamente l’affare, l’attività, la materia cui si riferisce la documentazione che raccoglie. È uno degli elementi distintivi tipici del fascicolo, al quale va posta la massima attenzione in sede di predisposizione, data la molteplicità dei profili in relazione ai quali può assumere rilevanza, anche nei confronti di terzi.

L’oggetto del fascicolo non deve, di norma, essere soggetto a variazioni nel corso del tempo e con il procedere della pratica cui si riferisce, onde attestare l’omogeneità e la coerenza nel trattamento della pratica stessa sin dal suo avvio. Eventuali variazioni possono, infatti, essere tracciate in altri appositi campi dedicati della copertina del fascicolo informatico: *Soggetti, Stato*, etc.

L’oggetto non deve essere troppo lungo e ciò per evitare il rischio di un appesantimento terminologico e complicare, anziché favorirne, la ricercabilità e la gestione nell’attività corrente e nel tempo successivo alla sua chiusura.

L’oggetto deve, inoltre, essere condiviso in primo luogo da tutti gli addetti della UO che prevalentemente ne farà uso, in modo tale da favorire una standardizzazione per UO a parità di tipologia di affare o di attività trattata.

#### **6.10. IL SOTTOFASCICOLO**

Il fascicolo può essere suddiviso in sottofascicoli.

Il sottofascicolo eredita le seguenti informazioni dal fascicolo in cui è aperto:

- l’anno di apertura;
- l’indice di classificazione;
- la visibilità (utenti e UO).



Valgono per il sottofascicolo le medesime regole indicate per il fascicolo (apertura e chiusura, oggetto, etc.).

### **6.11. CHIUSURA DEL FASCICOLO**

Il fascicolo è chiuso al termine del procedimento amministrativo, all'esaurimento dell'istruttoria, alla conclusione dell'attività cui si riferisce, ovvero su base temporale (per esempio alla fine dell'anno solare, quando concerne documentazione di fascicolo di attività).

La data di chiusura per il fascicolo di affare si riferisce generalmente alla data dell'ultimo documento inseritovi o alla data dell'inserimento stesso.

Il fascicolo è archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

## **7. GESTIONE IN SICUREZZA DEI DOCUMENTI INFORMATICI**

### **7.1. PRINCIPI GENERALI**

Il presente capitolo riporta le misure di sicurezza adottate nel sistema iShareDoc per la gestione, la trasmissione, l'accesso ai documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

Le misure di sicurezza in tale ambito 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 credenziali di accesso al sistema (utente e password) rappresentano il riconoscimento univoco del dipendente, in base ai requisiti di sicurezza.

### **7.2. MISURE GENERALI DI SICUREZZA PER LA GESTIONE DOCUMENTALE**

Le misure generali tecniche e organizzative inerenti il sistema iShareDoc, sono garantite dallo certificazione ISO/IEC 27001 riconosciuta al sistema stesso.

Per quanto riguarda la sicurezza della intranet dell'Ordine i criteri adottati sono i seguenti:

- protezione periferica della Intranet dell'Ordine;
- assegnazione ad ogni utente 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 periodica durante la fase di esercizio;
- gestione del servizio con particolare riferimento sia all'esecuzione e alla gestione delle copie di back-up dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino applicativo del sistema informatico;
- gestione, a cura del responsabile dei sistemi informativi, d'intesa con il responsabile della sicurezza, delle copie di back-up dei dati e dei documenti;



- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei “moduli” (patch e service pack) correttivi dei sistemi operativi;

I dati di operatività del personale registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di iShareDoc sono consultabili in caso di necessità dal RGD, o suoi delegati, ed è sottoposto a tracciamento.

### **7.3. FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA**

I documenti dell’Ordine sono prodotti con l’ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati previsti nel capitolo 2.

I documenti informatici prodotti dall’Ordine con altri prodotti di *editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard previsti nel capitolo 2 al fine di garantire la leggibilità mediante altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l’immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità, la sua riservatezza e la validazione temporale, il documento è sottoscritto con firma digitale o autografa.

### **7.4. GESTIONE DEI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA**

Questa sezione si riferisce alle attività svolte nell’ambito del sistema iShareDoc.

Il sistema che ospita i documenti informatici è configurato in modo tale da consentire:

- l’accesso esclusivo al server del sistema iShareDoc in modo che qualsiasi altro utente non autorizzato non possa accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l’identificabilità dell’utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Nell’ambito delle disposizioni del Manuale, nella gestione dei documenti informatici iShareDoc:

- garantisce la disponibilità, la riservatezza e l’integrità dei documenti e del registro di protocollo;
- garantisce la registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall’Ordine e gli atti dalla stessa formati al fine dell’adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente l’accesso in sicurezza alle informazioni del sistema da parte dei soggetti interessati;
- garantisce la corretta organizzazione dei documenti nell’ambito del sistema di classificazione d’archivio adottato.

#### **7.4.1. Componente fisica**

La componente fisica è ospitata in un centro servizi certificato ISO/IEC 27001 che garantisce standard qualitativi elevati nell’ambito della sicurezza informatica.

#### **7.4.2. Componente logica e infrastrutturale**

La componente logica e infrastrutturale dei sistemi di sicurezza gestisce l’integrità, la riservatezza, la disponibilità e il non ripudio dei dati, delle informazioni e delle trasmissioni.



Dal punto di vista architetturale la sicurezza è gestita dalle seguenti componenti:

- architettura multi-layer: consente di tenere separati i livelli funzionali di presentazione (presentation layer), dell'applicazione (application layer) e dei dati (data layer);
- i file dei documenti sono accessibili solo tramite il server di application layer;
- sicurezza del canale di comunicazione: i client che accedono all'archivio dei documenti e delle PEC comunicano tramite protocolli sicuri (HTTPS, SMTPS, POP3S).

Dal punto di vista applicativo la sicurezza è gestita dalle seguenti componenti:

- gestione di un insieme di profili di accesso attraverso i quali è possibile definire nel dettaglio cosa un utente può e non può fare nel sistema;
- possibilità di definire la visibilità dei documenti a livello di Registro, di tipologia documentale di fascicolo/sottofascicolo e di singolo documento;
- log applicativo delle attività svolte sul sistema con tracciamento di ogni operazione eseguita sul documento informatico e sul fascicolo ("storia" del documento/fascicolo).

#### **7.4.3. Gestione permessi per assegnazioni**

Il sistema gestisce la visibilità dei protocolli sulla base delle assegnazioni. Il documento nasce nel sistema con i permessi dell'utente o ufficio che lo sta protocollando, e poi sulla base delle assegnazioni la visibilità di accesso viene estesa dinamicamente alle persone ed uffici a cui è stata fatta l'assegnazione.

#### **7.4.4. Gestione della riservatezza**

Il sistema gestisce i livelli di riservatezza che possono essere utilizzati in combinazione con la "gestione permessi per assegnazioni" e che permettono di restringere ulteriormente la visibilità dell'oggetto e dell'allegato della registrazione di protocollo alle sole persone assegnate al livello di riservatezza e al responsabile del livello di riservatezza.

Il sistema gestisce più livelli di riservatezza, fra loro mutuamente esclusivi, consentendo di configurarne il numero e la denominazione.

Sono previsti due livelli di riservatezza così definiti:

- livello non riservato: a diffusione interna (relativo a documenti esportabili su internet e a documenti esportabili su intranet dell'Ordine);
- livello riservato: a consultazione limitata (relativo a documenti consultabili solo dalla UO di competenza).

Un documento di un certo livello è consultabile da tutti gli utenti aventi diritto di visibilità per quel livello e per lo specifico documento. L'abilitazione degli utenti ad accedere ai documenti con un certo livello di riservatezza è un diritto assegnato dall'amministratore del sistema.

#### **7.4.5. Gestione dei tracciamenti**

I tracciamenti di sicurezza sono costituiti da informazioni relative, ad es. ai dati o alle transazioni - presenti o transitate su iShareDoc - che è opportuno mantenere, poiché possono essere necessarie sia in caso di analisi e verifiche che abbiano ad oggetto le operazioni effettuate sul sistema, sia al fine di analizzare le cause di eventuali incidenti di sicurezza.

I tracciamenti di sicurezza sono costituiti da:

- log di sistema generati dal sistema iShareDoc;



- log dei dispositivi periferici del sistema (quali Intrusion Detection System - IDS, apparati di rete, firewall);
- registrazioni del protocollo;
- storia registrata delle operazioni effettuate nelle schede documentali del sistema iShareDoc.

I tracciamenti di sicurezza sono soggetti, in particolare, alle seguenti misure:

- i log di sistema sono tracciati nella storia delle registrazioni di protocollo e nelle schede documentali e archiviati a cadenza periodica;
- le registrazioni di protocollo sono conservate a cadenza giornaliera; il relativo registro giornaliero di protocollo è conservato come previsto nel paragrafo 5.2.

Le informazioni raccolte per controllare l'accesso al sistema sono quelle strettamente necessarie per l'identificazione dell'utente abilitato (userid).

#### **7.5. TRASMISSIONE DEI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA**

Come previsto dalla normativa vigente in materia di amministrazione digitale, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Il server di posta elettronica certificata del fornitore esterno (provider), di cui si avvale l'Ordine, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Per garantire al soggetto ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata di norma la firma digitale con la posta elettronica certificata a disposizione dei soggetti coinvolti nello scambio dei messaggi. Per i messaggi scambiati all'interno dell'Ordine mediante posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nelle procedure interne di sicurezza (cfr. A1 – Normativa di riferimento e bibliografia)

#### **7.6. ACCESSO AI DOCUMENTI INFORMATICI – ASPETTI DI SICUREZZA**

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso nominali (utente e password) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del sistema iShareDoc.

Le politiche di composizione, di aggiornamento e di sicurezza delle password sono configurate sui sistemi di accesso come obbligatorie, tramite il sistema iShareDoc.

Con specifico riferimento all'accesso e alle operazioni sui documenti e sulle schede documentali, iShareDoc:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;



- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore (storia della scheda documentale). Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Le password di accesso al sistema sono gestite all'interno di una struttura dati crittografata e accessibile soltanto da un processo di sistema.

#### **7.6.1. Profili di accesso**

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

- *Amministratore*, che ha la visibilità completa di tutti gli oggetti documentali del sistema, quali: schede, documenti, allegati, fascicoli, registri, etc.
- *Utente generico*, che ha la visibilità per competenza o per conoscenza delle schede documentali secondo i profili di assegnazione.

#### **7.6.2. Modalità di gestione delle utenze e dei relativi profili di accesso**

Al fine di procedere alla gestione delle utenze, l'Amministratore, sulla base delle richieste scritte pervenute ovvero sulla base degli Ordini di servizio e delle Comunicazioni al personale di carattere organizzativo, procede alla configurazione del sistema sia per la creazione sia per la disattivazione delle utenze con profilo di accesso *Utente generico*.

La creazione di nuove utenze di *Amministratore* è configurata di concerto con il responsabile della sicurezza informatica, che ne tiene traccia.

Le funzioni informatiche di interscambio con altri sistemi applicativi avvengono attraverso utenze amministrative la cui messa in sicurezza avviene di concerto con il responsabile della sicurezza informatica.

In caso di smarrimento della password, debitamente attestato da una richiesta scritta, l'Amministratore procede alla ridefinizione e alla riassegnazione di una nuova password all'utente. In qualsiasi momento e per un numero illimitato di volte l'utente, entrato nel sistema, può cambiare la propria password di accesso.

#### **7.6.3. Utenti interni**

Ciascun utente interno di iShareDoc può accedere solamente ai documenti e alle relative schede documentali a lui assegnati, ovvero assegnati al gruppo di appartenenza.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'Ordine. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono definiti dal RGD o da suoi delegati.

Ulteriori elementi di abilitazione al sistema sono descritti nell'ambito della procedura interna relativa alla riservatezza (cfr. A1 – Normativa di riferimento e bibliografia).

#### **7.6.4. Utenti esterni**

L'accesso al sistema iShareDoc da parte di soggetti esterni avviene per il tramite di sistemi di cooperazione applicativa, secondo gli standard e il modello architetturale basati su canali di comunicazione telematici gestiti dall'Ordine (quali: Portale Web e PEC).



Se la consultazione avviene in sede, di fronte all'interessato, l'istruttore ha cura della tutela della riservatezza dei dati presenti nel sistema. Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento possono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

L'eventuale accesso a iShareDoc da parte di utenti esterni è realizzato mediante l'impiego di sistemi sicuri di identificazione ed autenticazione e la profilazione di utenze nominali dedicate.

Agli utenti esterni riconosciuti ed abilitati alla consultazione dei dati propri presenti all'interno dell'Ordine sono fornite le informazioni necessarie per accedere a detti documenti amministrativi.

### **7.7. POLITICHE DI SICUREZZA ADOTTATE DALL'ORDINE**

Le politiche di sicurezza, come da procedure interne riportate in A1 – Normativa di riferimento e bibliografia, stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

Le politiche illustrate sono correlate alle responsabilità dirigenziali e dei dipendenti che sono adottate in caso di riscontrata violazione delle prescrizioni dettate in materia di gestione della visibilità e di accesso in sicurezza ai documenti informatici da parte di tutti gli utenti (interni ed esterni) che, a qualunque titolo, interagiscono con il sistema iShareDoc.

Il RGD, o suoi delegati, d'intesa con i responsabili della sicurezza, della tutela dei dati personali e dei sistemi informativi, procede al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

Il riesame delle politiche di sicurezza è conseguente al verificarsi dei seguenti casi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica che potrebbero incidere sugli obiettivi o sul livello di sicurezza complessiva;
- aggiornamenti delle prescrizioni normative;
- risultati delle attività di audit interni.

Di norma, tale attività è svolta con cadenza annuale.

### **7.8. MANUTENZIONE ORDINARIA ED AGGIORNAMENTI**

Allo scopo di garantire la continuità del servizio, si prevede un piano di manutenzione programmata del sistema utilizzato, a cura del fornitore del servizio.

### **7.9. GESTIONE DI EVENTI ECCEZIONALI**

Le linee generali delle modalità adottate per fronteggiare eventi eccezionali nell'ambito del processo di gestione dei sistemi sono quelle garantite dallo standard ISO/IEC 27001.

Le firme digitali utilizzate nel sistema sono apposte tramite dispositivo sicuro (*smart-card o chiavetta usb*). In caso di guasti a tale dispositivo, l'Ordine può avvalersi del supporto tecnico dell'ente certificatore, che è immediatamente contattato. Inoltre, è prevista la duplicazione del dispositivo di firma per i delegati.





## **8. CONSERVAZIONE DEI DOCUMENTI INFORMATICI**

### **8.1 AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE**

L'Ordine affida il servizio di conservazione a norma ad Unimatica Spa, Società accreditata presso l'Agenzia per l'Italia Digitale e il cui sistema di conservazione è conforme al DPCM 3 Dicembre 2013 Regole tecniche in materia di sistemi di conservazione e allo standard ISO 14721:2012 – Open Archival Information System (OAIS) reference model.

L'Ordine ha nominato, tramite Delibera del Consiglio, la società Unimatica Spa come Responsabile del servizio di conservazione, inoltre, nella sua qualità di titolare del trattamento dei dati, ha incaricato Unimatica Spa come Responsabile esterno del trattamento dei dati, ai sensi del D.Lgs. 196/2003 Codice in materia di protezione dei dati personali, relativamente e limitatamente ai trattamenti effettuati per conto dell'Ordine in particolare riguardanti la gestione e conservazione dei documenti come è indicato nella Delibera di affidamento.

### **8.2 COMPITI DEL RESPONSABILE DELLA CONSERVAZIONE**

Le procedure per i versamenti sono dettagliatamente descritte nelle specificità contrattuali definite dal Responsabile della Conservazione in accordo con il Responsabile del Servizio di Conservazione di Unimatica Spa.

Il ruolo del Responsabile della Conservazione è quello di monitorare le procedure di creazione ed invio dei Pacchetti di Versamento (PDV) in modo che siano rispettati gli accordi di servizio stabiliti. La creazione e l'invio dei PDV al sistema di conservazione di Unimatica Spa avviene in automatico attraverso il sistema iShareDoc.

Il Pacchetto di Versamento così prodotto viene inviato tramite Web Services e ad ogni PDV viene attribuito un codice univoco che ne permette l'identificazione certa all'interno del sistema di conservazione.

Il PDV viene lavorato dal sistema di conservazione di Unimatica Spa e trasformato in Pacchetto di Archiviazione. Le regole per la creazione e chiusura dei PDA sono stabilite precedentemente dal Responsabile della Conservazione in accordo con il Responsabile del Servizio di Conservazione di Unimatica Spa e dettagliate nelle specificità contrattuali.

Il Responsabile della Conservazione ha la possibilità di definire gli utenti che potranno visualizzare i PDA conservati da Unimatica Spa attraverso un portale web. Le credenziali di accesso a tale portale sono personali e rilasciate da Unimatica Spa agli utenti definiti nelle specificità contrattuali. In caso di necessità dal portale è possibile effettuare il download del Pacchetto di Distribuzione ed eventualmente anche delle prove di conservazione.



### 8.3 TIPOLOGIE DOCUMENTALI E RELATIVE TEMPISTICHE DI INVIO IN CONSERVAZIONE

Le tipologie documentali e le relative tempistiche di invio al sistema di conservazione di Unimatica Spa sono stabilite dal Responsabile della Conservazione in ottemperanza con quanto stabilito dalla Normativa vigente.

Di seguito i dettagli delle tipologie documentali e delle relative tempistiche di invio.

TIPOLOGIA DOCUMENTALE	TEMPISTICHE DI INVIO IN CONSERVAZIONE
Registro Giornaliero di protocollo	Entro la giornata lavorativa successiva <sup>1</sup>
Documenti protocollati	Entro la giornata lavorativa successiva alla protocollazione
Documenti non protocollati ma inseriti in appositi registri	Entro la giornata lavorativa successiva alla registrazione
Altri documenti	Il primo giorno lavorativo successivo al termine del mese precedente

**Tabella 1: Tipologie documentali e tempistiche di invio in conservazione**

L'elenco delle tipologie documentali e delle relative tempistiche di invio sarà aggiornato ogni volta in cui il Responsabile della Conservazione definirà nelle specificità contrattuali, in accordo con il Responsabile del Servizio di Conservazione di Unimatica Spa, una nuova tipologia documentale.

## 9. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE DI GESTIONE

### 9.1. MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO

Il Manuale, in sede di prima adozione, è approvato dal Consiglio dell'Ordine su proposta del RGD.

Il presente Manuale sarà aggiornato direttamente dal RGD a seguito di:

- sopravvenienze normative;
- introduzione di nuove prassi tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- evoluzione delle procedure ridefinite nello svolgimento delle attività correnti;
- evoluzione delle infrastrutture tecnologiche.

Per l'esecuzione di tali modifiche il RGD si avvale dei propri delegati, ovvero dei funzionari idonei per competenze ed esperienze.

Ogni altra modifica sarà sottoposta ad approvazione da parte del Consiglio dell'Ordine.

<sup>1</sup> DPCM 3 Dicembre 2013 Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82 del 2005.



## **9.2. PUBBLICITÀ DEL MANUALE**

Il presente Manuale, ai sensi dell'art. 22 della legge 7 agosto 1990, n. 241, è reso disponibile alla consultazione da parte del pubblico mediante pubblicazione sul sito Internet istituzionale, fatta eccezione per gli Allegati, stante il loro contenuto prettamente operativo. Inoltre copia del presente Manuale è:

- fornita a tutto il personale dell'Ordine mediante la rete intranet;
- inviata, per conoscenza, all'AgID, Agenzia per l'Italia Digitale.

## **9.3. ENTRATA IN VIGORE DEL MANUALE**

Le prescrizioni del presente Manuale trovano applicazione dal 1° ottobre 2015.



## **ADDENDA**



## **A1 – NORMATIVA DI RIFERIMENTO E BIBLIOGRAFIA**

### **1. Normativa generale su documento, protocollo e archivi**

**Legge del 7 agosto 1990, n. 241** e successivi aggiornamenti

*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*

**Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445**

*Disposizioni legislative in materia di documentazione amministrativa*

**Decreto legislativo del 30 giugno 2003, n. 196**

*Codice in materia di protezione dei dati personali*

**Decreto legislativo del 22 gennaio 2004, n. 42**

*Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*

**Decreto legislativo del 7 marzo 2005, n. 82** e successivi aggiornamenti

*Codice dell'Amministrazione digitale*

**Decreto del Presidente della Repubblica dell'11 febbraio 2005, n. 68**

*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*

**Decreto ministeriale del 2 novembre 2005**

*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*

**DPMC 30 marzo 2009**

*Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.*

**Delibera CNIPA, n. 45 del 21 maggio 2009**

*Regole per il riconoscimento e verifica del documento informatico.*

**Determinazione DigitPA n. 69 del 28 luglio 2010**

*Modifica alla Delibera n. 45/2009*

**D. lgs. 30 dicembre 2010, n. 235**

*Modifiche e integrazioni al decreto legislativo 7 marzo 2005, n. 82 "NUOVO CAD".*



**DigitPA, Circolare del 29 dicembre 2011, n. 59**

*Modalità per presentare la domanda di accreditamento da parte dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82*

**Agenzia per l'Italia Digitale, Circolare del 30 aprile 2013, n. 62**

*Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD*

**Agenzia per l'Italia Digitale, Circolare del 23 gennaio 2013, n. 60**

*Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni*

**DPCM 22 febbraio 2013**

*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli art. 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*

**Decreto del Presidente del Consiglio dei Ministri del 21 marzo 2013**

*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*

**Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013**

*Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005*

**Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013**

*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5- bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005*

**Circolare AGID 10 aprile 2014, n. 65**

*Modalità per l'accredito e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82*



**Decreto MEF 17 giugno 2014**

*Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005*

**Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014**

*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 bis, 23 ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

**2. Regolamentazione interna**

**Regolamento del procedimento amministrativo** (adottato dal Consiglio dell'Ordine con delibera del 27 gennaio 2014)

*Regolamento attuativo della legge 7 agosto 1990, n. 241 e successive modificazioni*

**Delibera del 21 settembre 2015**

*Approvazione del Titolario di classificazione*

**Delibera del Consiglio dell'Ordine 21 settembre 2015**

*Nomina del Responsabile per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi e del Responsabile della conservazione*

**Comunicazione al personale del 21 settembre 2015**

*iShareDoc - Dematerializzazione dei flussi documentali dell'Ordine: delega di funzioni per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi nonché per la conservazione documentale.*

**Documentazione di sicurezza 2015**

*Il Documento Programmatico sulla Sicurezza dei dati personali ai sensi del D. Lgs. n. 196/2003*





## A2 – GLOSSARIO

**Accesso:** Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti 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.

**Archivio:** Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto produttore durante lo svolgimento dell’attività.

**Archivio informatico:** Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.

**Conservazione dei documenti informatici:** 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.

**Copie autentiche di documenti:** v. “Copie di documenti”.

**Copie di documenti:** riproduzioni, totali o parziali, di documenti originali (v.). Le copie ottenute con qualsiasi procedimento che dia garanzia della riproduzione fedele e duratura del documento originale (cd. “copie autentiche”) possono essere validamente prodotte in luogo degli originali.

**Documento originale:** documento formato originariamente per rappresentare il suo specifico contenuto. Il documento analogico può essere originale “unico” (v.) e “non unico” (v.). Il documento cartaceo (v.) è originale quando è redatto nella sua versione definitiva, perfetta e autentica negli elementi sostanziali e formali del mittente e del destinatario, stampato su carta intestata e sottoscritto con firma autografa. Il documento informatico (v.) da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del CAD e alle regole tecniche previste dalle disposizioni di legge.

**Documento originale non unico:** documento analogico (v.) per il quale sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.

**Documento originale unico:** documento analogico (v.) che costituisce l’unica fonte del suo contenuto.

**Esibizione:** Operazione che consente di visualizzare un documento conservato e di ottenerne copia.

**Firma digitale:** particolare tipo di firma elettronica qualificata (v.) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e 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:** insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

**Firma elettronica avanzata:** firma elettronica (v.) ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con



mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce, in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

**Firma elettronica qualificata:** firma elettronica avanzata (v.) basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.

**Gestione documentale:** insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti nell'ambito del sistema di classificazione d'archivio adottato.

**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.

**Iter approvativo:** insieme di visti e firme necessari per approvare da parte dei ruoli d'Istituto competenti la corrispondenza in partenza prima che questa sia protocollata.

**Manuale della conservazione:** Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 del DPCM 3 dicembre 2013 Regole tecniche in materia di sistemi conservazione.

**Massimario di selezione:** 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 titolario 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 quarant'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.

**Memorizzazione:** Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.

**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; tale insieme è descritto nell'allegato 5 del presente decreto.

**Pacchetto di Archiviazione (PDA):** pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 Dicembre 2013, Regole tecniche in materia di sistema di conservazione, e secondo le modalità riportate nel manuale di conservazione.

**Pacchetto di Distribuzione (PDD):** pacchetto informativo inviato dal sistema all'utente in risposta ad una sua richiesta.

**Pacchetto di Versamento (PDV):** pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

**Posta elettronica certificata (PEC):** sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.



**Processo di conservazione:** Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche del sistema di conservazione.

**Registrazione di protocollo:** memorizzazione, per ogni documento ricevuto o spedito, delle informazioni riguardanti il documento stesso.

**Responsabile della conservazione:** Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM Regole tecniche in materia di sistema di conservazione.

**Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi:** dirigente/funziario a ciò preposto (v.).

**Responsabile del trattamento dei dati:** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

**Scheda documentale:** insieme di dati associati ad uno specifico documento informatico, con eventuali relativi allegati, che ne tipizzano gli elementi informativi, utili in fase di protocollazione, fascicolazione e ricerca.

**Segnatura di protocollo:** apposizione o associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

**Sistema di conservazione:** Sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD.

**Sistema di gestione informatica di 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 protocollo informatico:** insieme di programmi elaborativi e di archivi di dati che, insieme, costituiscono l'applicazione attraverso la quale l'Ordine assicura la gestione informatica della generalità dei propri documenti ex art. 52 del D.P.R. n. 445/2000.

**Soggetto produttore:** Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

**Tab:** indica una delle sezioni informative della scheda documentale del sistema iShareDoc in cui sono riportati i metadati e le informazioni relative ai documenti informatici.

**Unistorage:** Applicazione della società Unimatica per la gestione dei Servizi di Conservazione a Norma dei documenti digitali.



### **A3 – ABBREVIAZIONI, SIGLE E ACRONIMI DELL'ISTITUTO**

#### **Elenco delle abbreviazioni e sigle di area giuridica**

App / Cda	Corte d'Appello
Cciv	Cassazione civile
Cpen	Cassazione penale
CdS	Consiglio di Stato
CdC	Corte dei Conti
CNDCEC	Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
CTP	Commissioni tributarie provinciali
CTR	Commissioni tributarie regionali
CPGT	Consiglio di Presidenza della giustizia tributaria
Gip	Giudice per le indagini preliminari
Gup	Giudice dell'udienza preliminare
GdP	Giudice di pace
ODCEC	Ordine dei Dottori Commercialisti e degli Esperti Contabili
Pref	Prefetto
RG	ruolo generale
RGGip	ruolo generale del giudice per le indagini preliminari
RGNR	ruolo generale delle notizie di reato
TAR	Tribunale Amministrativo Regionale
Trib	Tribunale

#### **Provvedimenti normativi**

BUR	bollettino ufficiale regionale
BUniRic	bollettino università e ricerca
Cost	Costituzione
CC	Codice civile
CP	Codice penale
CS	Codice della strada
CPC	Codice di procedura civile
CPP	Codice di procedura penale
daCC	disposizioni per l'attuazione del codice civile e disposizioni transitorie
daCPC	disposizioni per l'attuazione del codice di procedura civile e transitorie
daCPP	disposizioni per l'attuazione del codice procedura penale e transitorie
dtf	disposizioni transitorie finali
Dir	Direttiva
DL	Decreto legge
DLgs	Decreto legislativo
DM	Decreto ministeriale
DPCC	Decreto del Presidente della Corte dei conti
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica



GU	Gazzetta ufficiale
L	Legge
LR	Legge regionale
Reg	Regolamento
TU	Testo unico

#### **Provvedimenti normativi specifici**

CAD	D.Lgs. 7 marzo 2005, n. 82 e successivi aggiornamenti
TUB	decreto legislativo 1° settembre 1993, n. 385 e successive modificazioni
TUF	D.Lgs. 24 febbraio 1998, n. 58 e successivi aggiornamenti - Testo unico delle disposizioni in materia di intermediazione finanziaria (Testo unico della finanza)

#### **Provvedimenti interni**

DEL	Delibera del Consiglio dell'Ordine
OdG	Ordine del Giorno
OdS	Ordini di Servizio

#### **Abbreviazioni fiscali**

CUD	certificazione unica dei redditi di lavoro dipendente
Fatt	fattura
IRAP	imposta regionale sulle attività produttive
IRPEF	imposta sul reddito delle persone fisiche
IRES	imposta sul reddito delle società
ISEE	indicatore della situazione economica equivalente
IVA	imposta sul valore aggiunto
Mod	modello
RA	ritenuta d'acconto
UNICO	modello unificato compensativo

#### **Altre abbreviazioni utili**

aa	anno accademico
abi	codice assegnato dall'Associazione Bancaria Italiana
ac	amministrazione controllata
aia	autorizzazione integrata ambientale
as	anno scolastico
art	articolo
BD	blu-ray disc
BE	back-end
c	comma
cab	codice di avviamento bancario
cap	codice di avviamento postale
ccb	conto corrente bancario
ccp	conto corrente postale



CD	compact disc
cd	cosiddetto
cf	codice fiscale
ci	carta di identità
cie	carta di identità elettronica
CIG	codice identificativo di gara
cig	cassa integrazione guadagni
co	presso
cs	carta dei servizi
DVD	digital versatile disc
EIP	ente di interesse pubblico
etc	eccetera
FE	front-end
FSE	fondo sociale europeo
Fto	firmato
Gdf	Guardia di finanza
HD	hard disk
IBAN	international bank account number
IFR	Indennità di fine rapporto
INI-PEC	Indice nazionale degli indirizzi PEC di professionisti e imprese
iPA	Indice delle Pubbliche Amministrazioni
inc	Incorporated
lca	liquidazione coatta amministrativa
ltd	Limited
mav	pagamento mediante avviso
n / nn	numero / numeri
OICVM	Organismi d'investimento collettivo in valori mobiliari
OPA	offerta pubblica di acquisto
OPS	offerta al pubblico di sottoscrizione
OPVS	offerta al pubblico di sottoscrizione e vendita
OPV	offerta al pubblico di vendita
PA	pubblica amministrazione
PDA	pacchetto di archiviazione
PDD	pacchetto di distribuzione
PDV	pacchetto di versamento
PEC	posta elettronica certificata
PEG	piano economico di gestione
PEO	progressione economica orizzontale
PEV	progressione economica verticale
Pi	partita IVA
PIN	personal identification number
PON	programma operativo nazionale
POR	programma operativo regionale



PTA	personale tecnico amministrativo
RTI	raggruppamento temporaneo di imprese
sa	società anonima
scarl	società cooperativa a responsabilità limitata
scpa	società cooperativa per azioni
SICAV	società di investimento a capitale variabile
SIM	società di intermediazione mobiliare
snc	società in nome collettivo
spa	società per azioni
srl	società a responsabilità limitata
TFR	Trattamento di fine rapporto
VAS	valutazione ambientale strategica
VIA	valutazione d'impatto ambientale
VIC	valutazione d'incidenza
SIC	sito di importanza comunitaria
UE	Unione europea
vs	contro (versus)
ZPS	zona di protezione speciale
ZTL	zona a traffico limitato





#### A4 – Scheda della ODCEC

<b>Denominazione dell'Ente</b>	Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma ODCEC di Roma
<b>Denominazione dell'Area Organizzativa Omogenea</b>	ODCEC di Roma
<b>Nominativo del Responsabile per la tenuta del Protocollo informatico, per la gestione dei flussi documentali e degli archivi</b>	Mario Valle
<b>Sito internet ufficiale della AOO</b>	<a href="http://www.odcec.roma.it">www.odcec.roma.it</a>
<b>Casella di posta elettronica istituzionale dell'AOO</b>	<a href="mailto:presidenza@pecodcec.roma.it">presidenza@pecodcec.roma.it</a>
<b>Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale</b>	Piazzale delle Belle Arti, 2 Via Flaminia, 141 00196 Roma Telefono (centralino) 06.367211
<b>Indirizzo completo della sede secondaria operativa a cui indirizzare l'eventuale corrispondenza convenzionale</b>	Via Petrella 4 00196 Roma
<b>Data di istituzione della AOO</b>	2008

#### A5 – UO DELL'ODCEC

##### FIGURE APICALI

Direttore (DIR)

##### UFFICI NON COORDINATI Sigla UO

Ufficio Amministrazione e Contabilità (UAC)

Segreteria di Presidenza (PRS)

Ufficio Albo e Tirocinio (UAT)

Ufficio Comunicazione e Formazione (FPC)

##### UFFICI COORDINATI Sigla UO

Ufficio Sistemi Informativi, Affari Generali e Protocollo (SIP)

Segreteria del Consiglio di Disciplina territoriale (CdD)



### **A6 – ELENCO PEC**

Nelle tabelle seguenti sono riportati tutti gli indirizzi di PEC attivate nell'Ordine e disciplinate nell'ambito del Manuale.

#### **PEC istituzionale e PEC relative alle UO**

<b>Indirizzo PEC</b>	<b>Unità organizzativa</b>
presidenza@pecodcec.roma.it	Indirizzo istituzionale - Segreteria di Presidenza
direzione@pecodcec.roma.it	Direzione
consigliodisciplina@pecodcec.roma.it	Segreteria del Consiglio di Disciplina Territoriale
albo@pecodcec.roma.it	Segreteria Albo, Elenco Speciale e Liquidazione Parcelle
tirocinio@pecodcec.roma.it	Segreteria Tirocinio e Registro Praticanti
formazione@pecodcec.roma.it	Ufficio Formazione Professionale Continua
amministrazione@pecodcec.roma.it	Ufficio Amministrazione e Contabilità
sistemi.informativi@pecodcec.roma.it	Ufficio Sistemi informativi

#### **PEC funzionali**

Sono attivati, infine, i seguenti indirizzi PEC "funzionali" dedicati a specifiche funzioni dell'Ordine,

<b>Indirizzo PEC</b>	<b>Attività – Unita Organizzativa</b>
protocollo@pecodcec.roma.it	Ufficio Protocollo



#### **A7 – Elenco dei documenti esclusi dalla registrazione di protocollo**

Sono escluse dalla protocollazione, ai sensi dell'art. 53. comma 5 del DPR n. 445/2000, le seguenti tipologie documentali:

- allegati, se accompagnati da lettera di trasmissione
- atti preparatori interni
- biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.)
- convocazioni ad incontri o riunioni e corsi di formazione interni
- delibere, disposizioni interne, ordini di servizio e comunicazioni al personale
- gazzette ufficiali, bollettini ufficiali PA
- giornali, riviste, libri
- materiali pubblicitari
- modulistica attinente a ferie, missioni, check-up, fornitura di materiali ed equipaggiamenti informatici, rapporti valutativi e documentazione simile
- atti notificati a mano ai dipendenti
- processi verbali
- ricevute di ritorno delle raccomandate A.R.



### A8 – Loghi, timbri, etichette

Si riporta alcuni esempio di loghi, timbri, etichette relativi ai documenti.

Etichetta di segnatura del protocollo in ingresso	 <p>Ordine Dott. Comm. Esp. Cont. - Roma Entrata - del 18/09/2015 11.38.15 - 23881</p>
Etichetta di segnatura del protocollo in uscita	 <p>Ordine Dott. Comm. Esp. Cont. - Roma Uscita - del 18/09/2015 12.02.50 - 23887</p>
Logo e indirizzi della busta in uscita	 <p><b>Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma</b></p> <p>Circondari dei Tribunali di Roma e Velletri Ente di Diritto Pubblico</p> <p>via Flaminia, 141 00196 Roma</p>
Timbro per la distinta di corrispondenza	



Timbro di sede con indirizzo (ad es. per cartoline A/R)	<p>Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma 00196 Roma - Piazzale delle Belle Arti, 2 SEGRETERIA DISCIPLINA</p> <p>Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma Via Flaminia, 141 - 00196 Roma Tel. 06.367211 - Fax 06.36721220</p>
Timbro di "Accettazione" in ingresso	