CONSOB

COMMISSIONE NAZIONALE
PER LE SOCIETA' E LA BORSA

MANUALE DI GESTIONE

LUGLIO 2014

Versione: *01*
Stato: *Definitiva*
Data: *01/07/2014*
Approvazione *Delibera n. 18956 del 25 giugno 2014*

INDICE

* * *

[omissis]

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).

Ai sensi dell'art. 4 del medesimo DPCM, al Responsabile della gestione è assegnato il compito di "predisporre lo schema del manuale di gestione" di cui, nel successivo articolo 5, sono indicati i contenuti minimi.

Il legislatore ha previsto quattro ambiti nuovi, riguardanti i *formati*, i *metadati*, la gestione dei *fascicoli informatici*, l'esistenza di particolari *registri* e forme di raccolte di dati anche personali.

Le novità introdotte con l'intervento normativo di fine 2013 non modifica impianto e scopi propri del Manuale di gestione, come indicati nel *modello* definito nel 2006 dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione – CNIPA (attuale Agenzia per l'Italia Digitale); modello che, pertanto, conserva tuttora la propria ragion d'essere.

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 agli utenti CONSOB e ai soggetti esterni che a diverso titolo interagiscono con essa.

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 la CONSOB.

Più in articolare, il Manuale disciplina:

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto con il protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del Titolario di classificazione e del massimario di selezione e di scarto;

- 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 sostitutiva 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'Istituto.

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 della Commissione Nazionale per le Società e la Borsa – CONSOB, ivi inclusa la procedura interna di gestione dei documenti definita in sede di avvio, a luglio 2013, della piattaforma di gestione dematerializzata dei flussi documentali.

La gestione documentale CONSOB 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

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.
- **Delegati**: personale CONSOB incaricato formalmente dal RSP per l'espletamento di funzioni previste dalla normativa vigente in materia di amministrazione digitale.
- **DEMACO**: Dematerializzazione atti CONSOB - sistema centrale e integrato di dematerializzazione, gestione documentale e protocollo informatico; applicativo acquisito dall'Istituto per implementare il servizio integrato di protocollo informatico e gestione dei flussi documentali.
- **Istituto**: Commissione Nazionale per le Società e la Borsa – CONSOB.
- **MdG**: Manuale di Gestione del protocollo informatico, dei documenti e degli archivi.
- **OdS**: Ordine di Servizio.
- **PA**: Pubblica Amministrazione.
- **PEC**: Posta Elettronica Certificata.
- **RdD**: Responsabile di Divisione, da intendersi quest'ultima quale UO.
- **RdP**: Responsabile del Procedimento - il dipendente che assume su di sè 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.
- **RSP**: 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.
- **Tab (o pagina)**: sezione della scheda documentale con un insieme di informazioni e metadati relativi al documento informatico.
- **UNC**: Ufficio non coordinato nell'ambito di Divisione .
- **UOP**: Unità Organizzative di registrazione di Protocollo - identificano gli uffici che svolgono attività di registrazione di protocollo. Nell'Istituto corrispondono al Protocollo e alle Segreterie di Divisioni e/o Uffici non coordinati.
- **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. Nell'Istituto corrispondono alle Divisioni, agli Uffici non Coordinati nell'ambito di Divisione e agli Uffici coordinati nell'ambito di Divisione.

- **UP**: Unità di Protocollo - è la principale UOP, funzionalmente allocata in ambito Consob nella Direzione Generale.

Per un elenco completo delle disposizioni rilevanti si veda A2 – Normativa di riferimento e bibliografia.

Per il Glossario si veda A3 – Glossario.

Per un elenco completo di abbreviazioni, sigle e acronimi si veda A4 – Abbreviazioni, sigle e acronimi dell'Istituto.

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'Istituto individua un'unica AOO denominata CONSOB (A5 – Scheda della CONSOB), composta dall'insieme delle UO da cui è caratterizzato il relativo assetto organizzativo e funzionale.

Le UO che, alla data di adozione del presente Manuale, afferiscono alla AOO sono riportate in A6 – UO della CONSOB, 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 e degli archivi e della conservazione

In ambito CONSOB, 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 Responsabile della Divisione Amministrazione .

È in facoltà del Responsabile di avvalersi della delega di funzioni a dipendenti dell'Istituto 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 DEMACO;
- aprire e chiudere il registro di protocollazione di emergenza;
- curare le attività registrazione di protocollo affinché, in caso di guasti o anomalie, ne sia ripristinata la funzionalità entro max ventiquattro ore 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'Istituto 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 d'Istituto, 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;
- proporre le modalità e le misure organizzative e tecniche di cui all'art. 3, comma 1, lettera e) delle Regole tecniche per il protocollo inerenti alla eliminazione di protocolli diversi dal protocollo unico;
- predisporre il piano di visibilità e accesso in sicurezza relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici 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 L4), 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 dei 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.

1.5.3. Il delegato per la conservazione

I compiti del delegato alla conservazione, fra quelli previsti e da svolgersi anche d'intesa con le altre figure responsabili previste dalla normativa di riferimento, sono:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, del che tiene evidenza, in conformità alla normativa vigente;
- gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
- generare il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicurare la verifica periodica, con cadenza non superiore a cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 delle Regole tecniche per la conservazione;
- predisporre il manuale di conservazione di cui all'art. 8 delle Regole tecniche per la conservazione e curarne 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 L4), il delegato è autorizzato ad accedere, ai fini della gestione del sistema, ai metadati dei documenti L4 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.

1.6. Unità responsabili delle registrazioni di protocollo

Nella CONSOB il sistema di protocollazione è:

- *unico a livello istituzionale*, cioè tutte le UO e gli utenti abilitati accedono al sistema DEMACO 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, il Protocollo svolge i compiti di UOP principale d'Istituto per la corrispondenza in entrata e di UOP secondaria per la corrispondenza in uscita. Le Segreterie delle Divisioni e degli Uffici non Coordinati svolgono i compiti di UOP secondarie per la corrispondenza in entrata e di UOP principali per la corrispondenza 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 RdD, i RdUNC ed i RdU 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 dalla Commissione ai sensi dell'art. 31 del Regolamento di Organizzazione e Funzionamento.
Nel caso in cui tale figura non sia presente, il Responsabile dell'UO individua i nominativi dei dipendenti delegati che lo sostituiscono in caso di assenza o impedimento. I RdU comunicano l'elenco al RdD, che lo approva. L'elenco è, quindi, trasmesso al Direttore Generale e alla Divisione Amministrazione.
I Responsabili di UO provvedono, altresì, ad aggiornare l'elenco a seguito di modifiche intervenute all'organico della Divisione/Ufficio.
In caso di assenza o impedimento del Responsabile, le assegnazioni sono indirizzate, nell'ordine o in base a specifiche istruzioni del Responsabile stesso, al relativo sostituto, come individuato nel suddetto elenco.

1.8. Atti di organizzazione

L'Istituto è, come già sopra rilevato, identificato come un'unica AOO.
In data 7 marzo 2013 è stata istituita la casella di Posta Elettronica Certificata istituzionale della CONSOB.
In data 21 maggio 2013 l'Istituto 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/dettaglioIstituto.php?cod_amm=consob

Con delibera n. 18554 del 29 maggio 2013 è stato approvato il Titolario di classificazione.
Con disposizione del Direttore Generale n. 10 del 12 giugno 2013 il Responsabile della Divisione Amministrazione 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 27 giugno tale Responsabile si è avvalso della delega di funzioni a dipendenti dell'Istituto in possesso dei necessari requisiti di competenza e professionalità tecnica.

Il sistema di gestione della corrispondenza e dei flussi documentali d'Istituto denominato DEMACO, comprensivo del protocollo informatico, fondato sull'integrazione delle tecnologie digitali per l'intero ciclo di gestione del documento e dell'archivio informatico - dalla sua formazione alla sua eliminazione o conservazione nel tempo - a rilevanza sia interna che esterna, è divenuto operativo a partire dal 1° luglio 2013.

A decorrere da tale data è stato istituito il sistema unico di dematerializzazione, protocollo informatico e gestione informatica dei documenti e degli archivi, ferme restando l'esigenza di registrazioni specifiche[1].

Dalla stessa data del 1° luglio 2013:

- non è più prevista la produzione di documenti originali su supporto cartaceo, ad esclusione dei casi individuati nel presente Manuale; pertanto, la documentazione ufficiale - sia interna sia indirizzata a soggetti esterni - è prodotta esclusivamente in DEMACO 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'Istituto (Allegato 4 – 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'Istituto avvengono in via esclusiva tramite la piattaforma DEMACO;
- la documentazione digitale informatica, non necessariamente protocollata, è inserita nella piattaforma DEMACO nell'apposito "Registro di lavoro" (cfr. capitolo 6);
- la documentazione riguardante la pubblicità, la trasparenza e la diffusione di atti e informazioni da parte dell'Istituto, ovvero la pubblicazione sul relativo sito, è gestita e archiviata mediante la piattaforma DEMACO negli appositi registri (cfr. capitolo 6).

[1] Quali il registro riservato del Presidente e il registro della Camera di Conciliazione e Arbitrato.

1.9. Posta elettronica certificata (PEC)

CONSOB 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 CONSOB è la seguente: consob@pec.consob.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.

Ciascuna Divisione e ciascun Ufficio non Coordinato sono dotati di una propria casella PEC. Sono attive, inoltre, PEC c.d. "funzionali", dedicate a specifiche funzioni dell'Istituto. In presenza di comprovate specifiche esigenze operative possono essere rilasciate nuove "caselle funzionali" dedicate.

Sono, infine, previste PEC "operative" per specifiche esigenze di servizio emerse già prima della messa in esercizio della piattaforma DEMACO.

L'elenco completo delle PEC d'Istituto è riportato in A7 – Elenco PEC.

1.10. Firma digitale

CONSOB 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 da CONSOB mediante i previsti uffici di registrazione (RAO) interni all'Istituto.
Tutti i dipendenti dell'Istituto 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 DEMACO 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 DEMACO 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'Istituto dalla conoscenza di fatti e documenti (cfr. A2 – Normativa di riferimento e bibliografia).
Ciascun dipendente può richiedere, relativamente ai documenti e alle informazioni presenti nell'archivio d'Istituto, 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. Diritto di accesso per fini amministrativi

In conformità alla normativa vigente, l'Istituto 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 n. 18388 del 28 novembre 2012, successivamente modificata con delibera n. 18628 del 31 luglio 2013, l'Istituto ha approvato il Regolamento generale sui procedimenti amministrativi della CONSOB, ai sensi dell'articolo 24 della legge 28 dicembre 2005, n. 262, e dell'articolo 2, comma 5, della legge 7 agosto 1990, n. 241 e successive modificazioni.
Il Regolamento è pubblicato sul sito dell'Istituto.
Per l'esercizio del diritto di accesso ai documenti è previsto che il soggetto di norma presenti richiesta formale tramite PEC.

1.12.3. L'accesso civico

E' 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.

1.12.4. Diritto di consultazione per ricerca storico-scientifica

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

1.12.5. Tutela dei dati personali

L'Istituto, 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'Istituto per la sicurezza dei dati sono riportate nel successivo capitolo 9.

In relazione alla protezione dei dati personali trattati, CONSOB 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, sostanziantesi 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 (CD-ROM, 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'Istituto nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico e privato.

2.3.2. Documenti in partenza

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

2.3.3. Documenti interni

Per documenti interni si intendono i documenti scambiati tra UO della CONSOB.
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 informatico, è necessario registrare questa tipologia di documenti interni nel "Registro di lavoro" (cfr. capitolo 6).

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'Istituto: definizione e regime giuridico

Per documento d'Istituto si intende ogni documento prodotto o acquisito dalla CONSOB nello svolgimento della propria attività istituzionale e/o nell'esercizio delle proprie funzioni.
I documenti d'Istituto sono prodotti e gestiti mediante sistemi informatici, come previsto dalla vigente normativa. La scheda documentale del sistema DEMACO è parte integrante del documento informatico prodotto in Istituto.

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

Inoltre, i documenti, i fascicoli e l'archivio dell'Istituto 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 d'Istituto;
- 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'Istituto 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'Istituto;
- 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);
- codice identificativo del destinatario o dei destinatari secondo l'Anagrafica d'Istituto;
- numero di riferimento a un procedimento/fascicolo precedente o corrente;
- oggetto del documento;
- testo del documento;
- firma o sigla del responsabile della immissione dei dati e/o del RdP e/o di RdD, RdUNC, RdU;
- numero e descrizione degli allegati;
- dati dell'Istituto (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'Istituto.

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

- il Responsabile di UO, ovvero il personale dei segreteria delle UO;
- il personale delle UO coinvolto nella redazione dei documenti;
- il personale con funzioni di Protocollo;
- il RSP 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'Istituto di alcune regole per la normalizzazione del campo "Oggetto" delle schede documentali DEMACO e del relativo documento principale, al fine di definire un archivio razionale e usabile.
A tal riguardo si rimanda ai dettagli operativi riportati in Allegato 5 – Gestione del campo Oggetto della scheda documentale.

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[2].

Le tipologie di formato principali adottate e gestite nel sistema dell'Istituto 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
- Sistemi telematici d'Istituto : DAT, IMU, IMT, NT, I01(formati testuali)
- 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 nell'archivio di "Predisposizione" e successivamente protocollato nel Registro di "Protocollo Ufficiale" ovvero archiviato in altro Registro dedicato a specifiche tipologie di documenti interni (cfr. capitoli 5 e 6).

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. Validità del documento amministrativo in arrivo

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

- *documenti analogici*;
- *documenti informatici* ricevuti su caselle PEC dell'Istituto e provenienti da caselle PEC[3], anche se privi della firma digitale;
- *documenti informatici* ricevuti tramite sistemi telematici (ad es. trasmissione elettronica di dati da parte di soggetti vigilati per adempimenti regolamentari).

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

---

[2] Sono utilizzati strumenti aperti per l'identificazione dei formati basati sul *mime-type* o sul *magic number*.

[3] Le caselle di PEC dell'Istituto sono configurate in modalità "chiusa", per cui possono ricevere solo da altre caselle PEC.

3. Flussi di lavorazione dei documenti in arrivo

Di seguito sono descritti i flussi di lavorazione dei documenti d'Istituto, 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'Istituto 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'Istituto intrattiene rapporti, il documento amministrativo può 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 rimuovibile[5] - 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'Istituto

Il documento ricevuto tramite la casella istituzionale di PEC (*consob@pec.consob.it*) è gestito automaticamente dal sistema DEMACO, che la assegna al Protocollo, il quale 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 al Protocollo accede, regolarmente ed almeno due volte al giorno, al sistema DEMACO per verificare la ricezione di eventuali nuovi messaggi ricevuti tramite PEC.

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

In ogni caso se il mittente, pure essendo censito, non ha l'indirizzo PEC in anagrafe Consob, l'addetto al Protocollo può censire l'indirizzo PEC istituzionale/aziendale/professionale/personale, risultante da pubblici elenchi[4], avendo cura di evitare ogni forma di duplicazione del soggetto.

[4] 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 – *i*PA (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'Istituto

L'operatore di Protocollo, 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 della CONSOB*", riportando l'oggetto del messaggio ricevuto.

3.2. Documento informatico ricevuto sulle altre caselle PEC divisionali, operative e funzionali

3.2.1. Documento di competenza della UO

Ogni Divisione e Ufficio NC dispone di una casella di PEC, gestita direttamente dal sistema DEMACO, che provvede alla registrazione di protocollo e all'assegnazione al Responsabile (senza notifica) e alla Segreteria della UO di destinazione (con notifica).

Il documento ricevuto nella casella PEC (divisionale od operativa) è gestito in automatico dal sistema che procede sia alla protocollazione che alla assegnazione della UO destinataria, se l'indirizzo PEC del mittente è già presente nell'anagrafica.
Qualora la PEC non sia gestita automaticamente, la stessa è resa disponibile agli addetti al Protocollo che provvedono a completare le operazioni di protocollazione ed assegnazione alla UO competente.

Il documento ricevuto nella casella PEC (funzionale) è gestito e protocollato all'interno di DEMACO da parte degli addetti alla protocollazione, senza l'ausilio di procedure automatiche del sistema.

Il personale addetto alle segreterie accede, regolarmente ed almeno due volte al giorno, al sistema DEMACO per verificare la ricezione di eventuali nuovi messaggi ricevuti tramite PEC.

3.2.2. Documento di competenza non esclusiva della UO

Il personale di Segreteria procede all'assegnazione anche alle altre UO eventualmente interessate. Se la corrispondenza è riservata, il RdD/RdUNC determina il livello di riservatezza e dispone il suo trattamento secondo la regolamentazione interna sulla riservatezza (cfr. A2 – Normativa di riferimento e bibliografia).

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

3.2.3. Documento non di competenza della UO

La Segreteria riassegna immediatamente la corrispondenza ad altra UO, ove risulti chiara la competenza di quest'ultima; in caso contrario provvede ad assegnarla al Protocollo, indicando nelle annotazioni "Al Protocollo per riassegnazione a UO di competenza".

3.3. Documento informatico ricevuto su casella e-mail convenzionale

Il documento ricevuto via e-mail nelle caselle CONSOB non certificate rilevante dal punto di vista istruttorio è trasformato, a cura del ricevente, in un documento formato PDF e, con il supporto

della Segreteria, inserito, classificato e fascicolato nel sistema DEMACO, indicando i suoi eventuali allegati. Il documento è protocollato dalla Segreteria della UO ricevente.

3.4. Documento informatico ricevuto a mezzo fax

Il documento informatico ricevuto a mezzo fax-server presso il Protocollo o presso le Segreterie è recapitato nella casella del Protocollo (o della Segreteria) sotto forma di documento elettronico. L'addetto del Protocollo o della Segreteria procede all'estrazione del file, al suo inserimento in DEMACO, 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.

3.4.1. Documento ricevuto dal Protocollo

Il servizio di fax-server istituzionale osserva gli orari di accettazione del Protocollo, salvo i casi in cui, per motivi di urgenza o riservatezza o su espressa richiesta dei responsabili delle Divisioni/Uffici NC, gli addetti al Protocollo procedano all'accettazione dei documenti pervenuti via fax anche al di fuori delle suddette fasce orarie.

Gli addetti al Protocollo di Roma e di Milano accedono alle caselle di arrivo/partenza dei fax-server di entrambe le sedi e concordano le modalità di gestione dei fax per assicurare la continuità del servizio.

3.4.2. Documento ricevuto dalle Segreterie di competenza della UO

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

3.4.3. Documento ricevuto dalle Segreterie di competenza non esclusiva della UO

Il personale di Segreteria procede alle operazioni di accettazione, protocollazione e assegnazione anche alle altre UO interessate.
Nel caso in cui il documento è ricevuto fuori orario, su espressa richiesta dei Responsabili delle Divisioni/Uffici NC, il personale di Segreteria procede alle operazioni di accettazione, protocollazione e assegnazione anche alle altre UO interessate.
Se il documento è riservato, il RdD/RdUNC determina il livello di riservatezza e dispone il suo trattamento secondo la regolamentazione interna sulla riservatezza (cfr. A2 – Normativa di riferimento e bibliografia).

3.4.4. Documento ricevuto dalle Segreterie non di competenza della UO

La Segreteria può riassegnare immediatamente la corrispondenza ad altra UO, ove risulti chiara la competenza di quest'ultima; in caso contrario tale corrispondenza è assegnata al Protocollo, indicando nelle annotazioni "Al Protocollo per riassegnazione a UO di competenza".

3.5. Documento informatico ricevuto su supporto rimovibile

Nei casi in cui, in allegato ad un documento analogico, siano inviati documenti digitali su supporti rimuovibili[5], il Protocollo procede alla protocollazione del documento analogico nonché allo

[5] Sono esclusi tra i supporti rimovibili i floppy disk di qualsiasi formato, oramai obsoleti, la cui produzione è stata

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

Il sistema DEMACO assegna con notifica i documenti protocollati provenienti da flussi telematici alla Segreteria della Divisione di competenza, specificata nel sistema telematico, la quale li assegna tempestivamente con notifica ai funzionari incaricati della gestione di tali flussi.

3.7. Documento analogico ricevuto presso il Protocollo e le Segreterie delle UO

L'accettazione della corrispondenza, consegnata a mano oppure trasmessa mediante raccomandata, posta semplice, corriere o telegramma, avviene, di norma, dalle 8.15 alle 13.30 e dalle 14.15 alle 16.30 per tutti i giorni lavorativi del calendario nazionale.

Le unità che ricevono i documenti in arrivo sono:

- Protocollo;
- Segreterie delle UO.

In caso di necessità, su espressa richiesta dei responsabili delle Divisioni/Uffici non coordinati, il personale abilitato procede all'accettazione di specifici documenti anche al di fuori delle fasce orarie sopra indicate.

3.8. Accettazione di documento analogico presso il Protocollo

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

Tipologia di corrispondenza	Trattamento
Corrispondenza indirizzata direttamente a Presidente, Commissari, Direttore Generale, Vice Direttore Generale, Segretario Generale	- la busta non è aperta - sono apposti i timbri di accettazione - è trasmessa alle Segreterie competenti
Corrispondenza riportante la dicitura "Riservato" o "Personale" o corrispondenza valutata come tale	- la busta non è aperta - sono apposti i timbri di accettazione - è trasmessa all'interessato
Corrispondenza che non rientra nei due casi precedenti	- la busta è aperta - sono apposti i timbri di accettazione - si procede all'assegnazione

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

---

interrotta dalla principali case di settore.

Il personale addetto al Protocollo procede all'accettazione svolgendo le seguenti operazioni:

Mezzo di ricezione	Verifiche	Operazioni
Consegna a mano	Verifica della completezza della documentazione (es. corretto destinatario, presenza sottoscrizione autografa).	Apposizione Timbro "ricevuto" sulla copia per ricevuta. Apposizione Timbro "consegnato" sulla prima pagina dell'originale.
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. Apposizione Timbro "ricevuto" sulla busta.
Raccomandata, lettera semplice		Apposizione Timbro "ricevuto" sulla busta.
Telegramma		Apposizione Timbro "ricevuto" sul registro previsto dal vettore. Apposizione Timbro "ricevuto" sulla busta.
Corriere		Apposizione Timbro "ricevuto" sul registro previsto dal vettore. Apposizione Timbro "consegnato" sulla prima pagina dell'originale.

Esaurite le operazioni relative all'accettazione, il personale addetto al Protocollo 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 Segreterie delle UO

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

Il personale di Segreteria valuta, in funzione dei carichi di lavoro e del grado di urgenza desumibile dalla documentazione ricevuta, se procedere direttamente alle operazioni di accettazione, protocollazione, segnatura di protocollo tramite timbratura riportante il numero di protocollo, scansione e assegnazione anche alle altre UO interessate oppure inoltrare il documento cartaceo al Protocollo.

Nel primo caso il documento cartaceo è trasmesso al Protocollo non appena possibile; nel secondo la Segreteria appone, prima della trasmissione del documento cartaceo al Protocollo, il timbro di accettazione.

Nel caso in cui il documento sia ricevuto fuori orario, su espressa richiesta dei Responsabili delle Divisioni/Uffici non coordinati, il personale di Segreteria procede alle operazioni di accettazione, protocollazione, segnatura di protocollo tramite timbratura riportante il numero di protocollo, scansione e assegnazione. Ove la competenza non sia esclusiva della UO, la stessa Segreteria assegna il documento anche alle altre UO interessate.
Se il documento non ha carattere di riservatezza, l'originale cartaceo è trasmesso al Protocollo il giorno lavorativo seguente.
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 al Protocollo, previa apposizione del timbro di accettazione.

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 al Protocollo procede all'accettazione, alla protocollazione e all'assegnazione senza la scansione. Il documento cartaceo è assegnato alla Segreteria della 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 Divisione master.
Qualora il documento sia munito di una lettera accompagnatoria, il Protocollo la scansiona e la invia alle Divisioni assegnatarie in formato digitale tramite DEMACO.

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 Divisioni, 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, Commissari, Direttore Generale, Vice Direttore Generale, Segretario Generale o RdD nonché i documenti classificati a livello 4 di riservatezza.

Modalità di trattamento
Il documento è accettato dal Protocollo e trasmesso in busta chiusa al destinatario. Ove il destinatario (Presidente, Commissari, Direttore Generale, Vice Direttore Generale, Segretario Generale, RdD), presa visione del documento, lo ritenga, dispone per l'invio del documento originale e della relativa busta al Protocollo, eventualmente con le indicazioni relative all'assegnazione ad altre UO ed al livello di riservatezza. Il Protocollo 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 elettronico, il Protocollo 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 con conseguente trasmissione al Protocollo.

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 DEMACO, la classificazione e la fascicolazione è eseguita dall'Ufficio competente, ovvero dalla relativa Segreteria.

3.10.5. Documentazione acquisita nel corso di ispezioni

Modalità di trattamento

Il materiale acquisito nel corso di ispezioni viene scansionato ed è acquisito in un database dedicato. La relazione ispettiva, ivi inclusi gli eventuali relativi allegati, è predisposta in formato elettronico, firmata digitalmente ed allegata alla nota di trasmissione; la nota è protocollata ed inviata alla UO committente. L'eventuale documentazione allegata è trasmessa in allegato alla scheda documentale, ovvero su supporto esterno non modificabile che può includere copia della stessa nota. Di tale trasmissione è fornita indicazione nelle annotazioni della scheda documentale della relazione ispettiva.

3.10.6. Documenti non attinenti alle attività dell'Istituto

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 Consob, con data e firma e con 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 DEMACO.

3.12. Smistamento e assegnazione alle UOP

Lo smistamento dei documenti all'interno dell'Istituto avviene, di norma, attraverso il sistema DEMACO, mediante assegnazione all'UO Master e ad eventuali UO cointeressate.
Contestualmente l'assegnazione avviene con visibilità per competenza alle Segreterie della UO master e delle altre UO assegnatarie e con visibilità per copia conoscenza ai relativi responsabili delle UO.

L'assegnazione avviene automaticamente con notifica alla Segreteria delle UO assegnatarie e senza notifica ai relativi Responsabili.

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 CONSOB 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 Divisioni/Uffici Non Coordinati avviene esclusivamente attraverso l'operazione di assegnazione di documenti firmati digitalmente e protocollati, sulla cui scheda documentale è possibile aggiungere annotazioni relative al documento stesso.

In caso di trasmissione all'Ufficio Segreteria della Commissione, il documento è spedito con notifica sia alla segreteria dell'Ufficio Segreteria della Commissione sia all'Ufficio Segreteria della Commissione.

L'assegnazione a Presidente, Direttore Generale, Vice Direttore Generale e Segretario Generale avviene:

- 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 delle Divisioni interessate;
- 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 al Protocollo li consegnano al personale incaricato che provvede alla consegna alle 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. Sotto-assegnazione

L'attività di sotto-assegnazione del documento in arrivo è svolta di norma dal personale della Segreteria della UO assegnataria, ovvero dal personale addetto alla protocollazione.

Per tale attività sono previste due modalità:

- *Assegnazione per visibilità*, che consente di estendere la visibilità del documento assegnato per competenza o per copia conoscenza, ovvero con o senza notifica;
- *Assegnazione per lavorazione*, disponibile ai Responsabili di UO e alle relative Segreterie, che consente, oltre ad estendere la visibilità del documento assegnato, di tracciare tale assegnazione in un'apposita "cassetta" della posta DEMACO, con la contestuale definizione di una scadenza e di un messaggio di assegnazione.

L'assegnazione senza notifica consente la visibilità del documento nel sistema (ad es. tramite ricerca), ma non richiede alcuna operatività all'assegnatario.

L'attività di assegnazione avviene, di norma, all'Ufficio di competenza, mentre l'assegnazione ai singoli utenti è effettuata per apporre il "visto/firma digitale" previsto dal sistema oppure per competenza all'istruttore della pratica (sia al responsabile di procedimento che all'assegnatario).

Qualora il documento richieda la valutazione del responsabile della UO, è assegnato con notifica dalla Segreteria al Responsabile di Divisione/Ufficio non coordinato, il quale:

- individua il livello di riservatezza e lo imposta ovvero dispone per la impostazione ad opera della Segreteria;
- individua gli uffici di competenza e provvede all'assegnazione ovvero assegna alla Segreteria fornendo disposizioni per l'assegnazione, anche attraverso l'impiego delle annotazioni elettroniche previste dal sistema.

Qualora il documento riporti elementi certi di assegnazione (quale, ad esempio, il numero di fascicolo-procedimento), la Segreteria può operare la sotto-assegnazione direttamente con notifica al Responsabile dell'ufficio e al Responsabile dell'istruttoria.

La Segreteria può, inoltre, operare in autonomia le sotto-assegnazioni per i documenti per i quali il Responsabile della Divisione/Ufficio NC abbia impartito formali direttive o istruzioni.

Qualora il livello di riservatezza sia pari o inferiore a L2, a meno di eccezioni indicate dal RdD/UNC, l'assegnazione avviene con notifica al responsabile dell'ufficio e in visibilità senza notifica agli addetti all'ufficio.

Per i documenti L3 e L4 l'assegnazione avviene con notifica al solo RdU, in base a quanto previsto dalla regolamentazione interna in materia di riservatezza. Il RdU provvede all'assegnazione con notifica del documento ai funzionari interessati.

La visibilità rimane inalterata per coloro ai quali fa capo la gestione dei documenti protocollati, quali il RSP e suoi delegati.

Le attività di assegnazione sopra rappresentate possono essere effettuate, con le medesime modalità e criteri, anche per il fascicolo informatico, ad esempio in caso di assegnazione di procedimenti 241. In questo caso l'assegnazione del fascicolo può avvenire con o senza l'estensione della visibilità dei relativi documenti.

3.14. Classificazione e fascicolazione

L'istruttore al quale è stato assegnato un documento provvede a classificarlo secondo il Titolario dell'Istituto (cfr. A10 – Titolario di Classificazione) e a fascicolarlo secondo i principi e i criteri indicati nel capitolo 7 ed in base al Piano di Fascicolazione (Allegato 4 – Piano di Classificazione e Fascicolazione archivistica).

4. Flussi di lavorazione dei documenti in partenza e a rilevanza interna

Di seguito sono descritti i flussi di lavorazione dei documenti inviati dall'Istituto, 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 esclusivamente di tipo informatico e sono trasmessi in via telematica attraverso le funzionalità di DEMACO. Il sistema è utilizzato per lo scambio di corrispondenza interna, sia formale che informale.

I documenti archiviati prima dell'avvio del processo di dematerializzazione (1° luglio 2013) 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 della relativa scheda documentale e si conclude con il consolidamento dello stesso in formato PDF.

Nel corso della fase di predisposizione l'istruttore:

- inserisce una nuova scheda documentale nel registro di Predisposizione;
- valorizza i metadati del tab indici della scheda documentale, specifica il livello di riservatezza e seleziona i destinatari per competenza/conoscenza;
- indica quale modalità va utilizzata per l'invio al destinatario qualora l'Istituto non disponga in anagrafe dell'indirizzo PEC del destinatario;
- crea il documento, anche attraverso la selezione di una tipologia documentale standard o ricorrendo ad un modello presente in DEMACO, lo associa alla scheda documentale e procede alla sua predisposizione.

I metadati della scheda documentale in fase di predisposizione del documento, sia per le "Comunicazioni in uscita" che per le "Comunicazioni Interne", sono:

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Archivio	Registro di Predisposizione	Lista	Sì	Sì
Tipo documento	Tipologia documentale correlata al protocollo in predisposizione: Comunicazione in uscita o Interne	Lista	Sì	Sì
Numero documento	Numero progressivo univoco della scheda documentale	Numerico	Automatico	Sì
Data documento	Data di creazione del documento	Data	Automatico	Sì
Titolo/ Classe	Classificazione in base al Titolario d'Istituto	Lista	Sì	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Lista (L0-L4)	Sì	Sì

Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	Sì	No
Tipo Comunicazione	Comunicazione per l'esterno o per l'interno	Lista	Sì	Sì
Diffusione interna	Indica se il documento è a diffusione interna (quale CaP: Comunicazioni al Personale)	Lista (flag SI/NO)	Sì	Sì
Stato	Stato del flusso di lavorazione in base al processo di workflow (quale protocollazione, archiviazione)	Testo (fase del processo)	Automatico	No
Data documento	Data del documento principale	Data	Sì	No
Tipo Vettore in assenza PEC	Vettore alternativo da utilizzare in mancanza dell'indirizzo PEC del destinatario	Lista (vettori)	Sì	Sì
Tipo Firma	Firma digitale, Firma autografa (Presidente_DG), Firma digitale (senza invio PEC)	Lista	Sì	Sì
Numero Sird	Riferimento ad eventuali pratiche, presenti nel sistema interno Sird, relative al documento protocollato	Testo	Sì	No
Modello	Modello documentale utilizzato precaricato dal sistema in automatico	Lista	Sì	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	Sì	Sì
Tab Anagrafica	Indica il mittente o il destinatario e/o il soggetto interessato.	Lista (Anagrafe)	Sì	Sì
Tab Documento	Include il documento principale della scheda, predisposta dal sistema in base al dato indicato nel Modello	Documento	Sì	Sì
Tab Allegati	Include uno o più documenti allegati (esterni e/o interni) alla scheda, con una descrizione per documento allegato ufficiale o non ufficiale	Documento	Sì	No
Tab Annotazioni	Riporta informazioni e note dell'utente utili a fini della protocollazione, archiviazione, trattamento dell'atto	Testo	No	No
Tab Visibilità	Indica la visibilità definita per la scheda documentale	Lista	Sì	No

Qualora il documento abbia un contenuto di interesse di più UO, a pari livello di responsabilità, procederà alla sua classificazione la prima UO firmataria, che è da considerarsi sempre master. Ciascuna UO potrà eventualmente fascicolare il documento all'interno dei propri fascicoli.

Qualora il documento non sia riservato, ovvero non è a diffusione pubblica (L0) o interna (L1), il funzionario che lo predispone, di norma, assegna allo stesso il livello di riservatezza L2.
In sede di predisposizione del documento informatico, il sistema automaticamente estende la visibilità della scheda documento a tutti gli addetti dell'ufficio, ad eccezione dei documenti predisposti direttamente dal responsabile della UO, la cui visibilità non viene estesa in automatico.

Qualora il documento afferisca a pratiche riservate, ad esso deve essere assegnato il livello 3 o 4 e la visibilità deve essere limitata al RdD, al RdU e agli istruttori che operano sullo stesso documento. Se la visibilità è rimossa a tutti gli utenti o uffici, il documento resta accessibile solo all'amministratore.

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/A, rendendolo altresì immodificabile, e assegnato ai responsabili per il visto elettronico e/o la firma digitale.

4.2. Approvazione

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

- il Presidente;
- il Direttore Generale;
- il RdD;
- il RdU;
- il RdP;
- altro soggetto specificamente ed espressamente individuato.

Sono abilitati anche i relativi sostituti.

Il visto elettronico dei documenti ha valore esclusivamente amministrativo all'interno dell'Istituto e va apposto solo ove previsto dalle vigenti disposizioni interne.

L'istruttore assegna il documento ai firmatari. Al termine della raccolta delle firme l'istruttore assegna il documento alla Segreteria per la protocollazione e l'invio al destinatario.

4.3. Registrazione di protocollo e relativa segnatura

La protocollazione di un documento in partenza è, di norma, eseguita dalla Segreteria della UO; tale funzione può essere svolta anche da altri addetti previa abilitazione autorizzata dal RSP 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, la Segreteria verifica se il destinatario presente nel tab "Anagrafica" della scheda documentale disponga di indirizzo PEC. In caso contrario, può censire l'indirizzo PEC istituzionale/aziendale del destinatario - risultante da pubblici elenchi - nell'Anagrafe dell'Istituto, avendo cura di evitare la duplicazione del soggetto.

La Segreteria o gli abilitati attivano il processo di protocollazione. Il sistema in automatico assegna il documento ai destinatari interni indicati nella scheda documentale del documento ovvero provvede all'invio della PEC ai destinatari esterni qualora si disponga dell'indirizzo PEC.

La ricevuta di consegna della PEC è automaticamente inserita nella medesima scheda documentale del documento in uscita nell'apposito tab "Pec".

Attraverso la consultazione del tab "Pec" della scheda documentale del protocollo in uscita, gli addetti alla protocollazione verificano la regolare ricezione della PEC da parte dei destinatari, ovvero se è stata recepita nel sistema la ricevuta di consegna della PEC. In caso contrario è possibile reiterare l'invio della PEC attraverso un'apposita funzione disponibile nel medesimo tab "Pec" della scheda documentale[6]. 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[7], la trasmissione non è effettuata e il sistema DEMACO invia un messaggio all'addetto alla protocollazione che ne dovrà dare immediata comunicazione al funzionario istruttore per le successive operazioni di invio[8].

Qualora l'indirizzo PEC del destinatario non sia presente nel tab "Anagrafica", 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) in Anagrafica[9]. Tale indirizzo estemporaneo sarà esclusivamente utilizzato per la trasmissione della specifica scheda documentale e riportato nel tab "Anagrafica" della scheda; al fine di evitare duplicazioni, non verrà trasferito nell'anagrafe CONSOB 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, il sistema utilizza per l'invio il canale indicato nel campo "Tipo vettore in assenza di PEC".

Qualora sia necessario materializzare il documento presso il Protocollo, il dato "Tipo Firma" deve essere impostato con il valore "Firma digitale". Il Protocollo prende in carico il processo di protocollazione, provvede alla materializzazione e termina il processo.

Qualora il documento debba essere protocollato e gestito direttamente dalla UO, il dato "Tipo Firma" va impostato con il valore "Firma digitale (senza invio PEC)"; il documento protocollato resta in carico alla UO e deve essere gestito in base alle proprie esigenze operative ovvero secondo le modalità impostate per il dato "Tipo vettore in assenza di PEC".

---

[6] Solo nel caso in cui l'invio tramite PEC non fosse andato a buon fine, è possibile effettuare l'invio con vettori alternativi (quali ad es. Raccomandata A/R, Fax)

[7] In base alla normativa vigente, il limite prevede una dimensione massima complessiva dei documenti allegati alla PEC, anche in base al numero dei destinatari.

[8] In caso di necessità e urgenza interviene l'amministratore del sistema facendo inviare più PEC con gli allegati previsti nella comunicazione in uscita, ovvero dispone la produzione di un CD/DVD come allegato alla lettera in uscita che viene materializzata.

[9] Inserire almeno i dati "Descrizione" (es. denominazione univoca del soggetto) e "Intestazione" (es. codice Consob), oltre all'indirizzo della PEC operativa.

Nel caso di invio per "e-mail" (non certificata) [10] o "pubblicazione web", l'UO che ha protocollato provvede a scaricare (*download* del file) il documento da DEMACO e a trattarlo secondo la modalità prescelta. Ancora, nel caso di "consegna a mano" (o negli altri casi di materializzazione del documento) la materializzazione resta a carico della UO che ha emesso il protocollo.

Qualora si tratti di invio di documenti interni, il sistema li assegna automaticamente alla UO di destinazione con notifica alla Segreteria della UO stessa e senza notifica al Responsabile della UO (RdD / RdUNC).

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 dal campo "*Tipo vettore in assenza di PEC*" 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. L'attestazione della conformità prevede l'inserimento delle informazioni di cui all'Allegato 2 – Procedure operative di formazione e gestione di alcune tipologie documentali.

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.

La distinta è inserita nel sistema DEMACO nel Registro di lavoro.

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

[10] Nei casi in cui il documento è trasmesso via e-mail, la segreteria della UO ovvero gli altri addetti della UO provvedono alla trasmissione in tal senso. Poiché l'attività è svolta dalla UO competente, il Protocollo non è chiamato a svolgere alcuna operazione.

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 presenta agli addetti al Protocollo la distinta di avvenuta spedizione dei plichi, che sarà verificata, scansionata e archiviata presso il Protocollo per un periodo di un anno.

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 segreterie, ricevuta la cartolina, provvedono alla scansione della stessa e la allegano alla relativa scheda documentale. Al termine dell'anno solare le cartoline vengono trasmesse al Protocollo.

4.5.2. Spedizione a mezzo fax

In caso di invio tramite fax, l'addetto al Protocollo rileva il fatto dal dato "*Tipo vettore in assenza di PEC*". 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 al Protocollo 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 protocollazione materializzano il documento, ne attestano la conformità e procedono alle successive operazioni di consegna a mano al destinatario.

Di norma, la consegna di documenti ai dipendenti avviene telematicamente tramite il sistema DEMACO. In presenza di particolari fattispecie operative, la Segreteria della UO provvede alla materializzazione del documento come precedentemente descritto e il Responsabile della UO, o un suo sostituto, procede all'attestazione di conformità. Il documento è successivamente consegnato all'interessato a cura di un addetto della Segreteria.

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

4.5.4. Spedizione corrispondenza interna tra le due sedi di Roma e Milano

Per una razionale gestione della spedizione di documenti interni tra le sedi di Roma e Milano dell'Istituto, sono impartite delle disposizioni operative interne (cfr. A2 – Normativa di riferimento e bibliografia) per il Protocollo, finalizzati all'espletamento di operatività inerenti sia la presa in carico, la preparazione e la spedizione della documentazione sia le attività finali concernenti la ricezione e la verifica di conformità dei plichi oggetto di trasmissione.

4.6. Procedure operative di formazione e gestione di alcune tipologie documentali

La procedura operativa per la formazione e la gestione digitale di alcune tipologie documentali è descritta nell'Allegato 2 – Procedure operative di formazione e gestione di alcune tipologie documentali. In tale allegato sono indicate le modalità operative in ambiente DEMACO per il trattamento delle seguenti principali tipologie di documenti:

- Documenti da sottoporre alla firma del Presidente o del Direttore Generale;
- Note informative per il Presidente;
- Disposizioni a firma del Presidente o del Direttore Generale;
- Ordini di Servizio;
- Comunicazioni al Personale;
- Relazioni per la Commissione;
- Deliberazioni;
- Notificazioni;
- Esposti;
- Istanze di accesso agli atti;
- Reportistica di assegnazione lavori.

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 del Protocollo e delle segreterie. Tuttavia, previa richiesta di abilitazione formulata dal RdD/RdUNC al RSP, o ad un suo delegato, altri addetti della UO possono essere abilitati a protocollare documenti in entrata.

5.1. Unicità del protocollo

Nell'ambito della CONSOB il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica, indipendentemente dal modello organizzativo adottato dall'Istituto.

Il Registro informatico ufficiale di protocollo è denominato in DEMACO "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[11];
- 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.

La documentazione che non è stata registrata dagli addetti della UOP o dal RSP, o delegati, è da considerarsi non valida .

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.

[11] In caso di ricezione multipla dello stesso documento, si inserisce un'annotazione nella scheda documentale del documento protocollato: *"Documento pervenuto per errore in copia multipla"*.

5.2. Registro giornaliero di protocollo

Il RSP, 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 trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

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

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Archivio	Registro Giornaliero	Testo	Automatico	Sì
Tipo documento	Scheda Registrazioni	Testo	Automatico	Sì
Progressivo	Numero identificativo assegnato in automatico al documento	Numerico	Automatico	Sì
Data Registrazione	Data assegnata in automatico al momento della generazione del registro giornaliero di protocollo	Data	Automatico	Sì
Nome File	Descrizione assegnata in automatico dal sistema al momento della generazione del registro giornaliero	Testo	Automatico	Sì
Tab Documento	Include il documento di registro giornaliero generato in automatico dal sistema e firmato dal RSP o delegato	Documento	Automatico	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'Istituto (ricevuti, trasmessi, interni formali, informatici e analogici).
Su ogni documento ricevuto o spedito dall'Istituto 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 e, comunque, sono effettuate entro i termini previsti per la conservazione digitale del documento stesso (cfr. capitolo 8).

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

Protocollo in ingresso

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Archivio	Registro di Protocollo Ufficiale	Testo	Automatico	Sì
Tipo documento	Tipologia documentale relativa al Registro: Protocollo in ingresso	Testo	Automatico	Sì
Numero Protocollo	Protocollo assegnato in automatico al documento	Numerico	Automatico	Sì
Data Protocollo	Data assegnata in automatico al momento del processo di protocollazione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	Sì	Sì
Protocollo emergenza	Eventuale protocollo di emergenza riversato in base alla procedura	Numerico	Sì	No
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Lista (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Data documento	Data del documento principale	Data	Sì	No
Assegnazione master	Prima UO assegnataria per competenza del protocollo	Testo	Sì	Sì
Altre UO assegnatarie	Altre UO assegnatarie del protocollo, nel caso di multiassegnazione	Testo	Sì	No
Data ricezione	Data di arrivo del documento. Metadato disponibile in caso di Protocollo in ingresso.	Data	Sì	No
Data Timbro Postale	Data del timbro postale riportata sul plico documentale. Metadato disponibile in caso di Protocollo in ingresso.	Data	Sì	No
Tipo Vettore	Vettore della comunicazione. Metadato disponibile in caso di Protocollo in ingresso.	Lista (vettori)	Sì	Sì
Riferimento Esterno	Indica l'eventuale numero di protocollo che figura sui documenti ricevuti. Metadato disponibile in caso di Protocollo in ingresso.	Lista	Sì	No
Numero Sird	Riferimento ad eventuali pratiche, presenti nel sistema interno Sird, relative al documento protocollato	Testo	Sì	No
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Tab Anagrafica	Indica il mittente del protocollo e/o il soggetto interessato o coinvolto (quali il soggetto vigilato; un dipendente, etc.).	Lista (Anagrafe)	No	Sì
Tab Documento	Include il documento principale del protocollo	Documento	No	Sì
Tab Allegati	Include uno o più documenti allegati ufficiali al protocollo, con una descrizione per documento allegato (interno e/o esterno). E' possibile aggiungere allegati non ufficiali.	Documento	No	No
Tab Annotazioni	Riporta informazioni e note dell'utente utili a fini di protocollo, di archiviazione e di trattamento dell'atto	Testo	No	No
Tab Visibilità	Indica la visibilità definita per la scheda documentale	Lista	Sì	Sì

Protocollo in uscita

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Archivio	Registro di Protocollo Ufficiale	Testo	Automatico	Sì
Tipo documento	Tipologia documentale relativa al Registro: Protocollo in uscita	Testo	Automatico	Sì
Numero Protocollo	Protocollo assegnato in automatico al documento	Numerico	Automatico	Sì
Data Protocollo	Data assegnata in automatico al momento del processo di protocollazione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	Sì	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Protocollo emergenza	Eventuale protocollo di emergenza riversato in base alla procedura	Numerico	Sì	No
Tipo comunicazione	Comunicazione per l'esterno o per l'interno	Testo	No	Sì
Diffusione interna	Indica se il documento è a diffusione interna (quale CaP: Comunicazioni al Personale).	Testo (flag SI/NO)	No	Sì
Data documento	Data del documento principale	Data	Sì	No
Tipo vettore in assenza PEC	Vettore di comunicazione con destinatario privo di PEC.	Lista	Sì	Sì
Tipo firma	Firma digitale, Firma autografa, Firma digitale (senza invio PEC).	Lista	No	Sì
Numero Sird	Riferimento ad eventuali pratiche, presenti nel sistema interno Sird, relative al documento protocollato	Testo	Sì	No
Divisione \UnC Mittente	UO mittente di primo livello del Protocollo in uscita.	Testo	Sì	Sì
Ufficio Mittente	UO mittente di secondo livello del Protocollo in uscita	Testo	Sì	No
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì
Tab Anagrafica	Indica il mittente o il destinatario del protocollo e/o il soggetto interessato o coinvolto (quali il soggetto vigilato; un dipendente, etc.).	Lista (Anagrafe)	No	Sì

Nome dato	Descrizione	Tipo	Modificabile	Obbligatorio
Tab Documento	Include il documento principale del protocollo	Documento	No	Sì
Tab Allegati	Include uno o più documenti allegati ufficiali al protocollo, con una descrizione per documento allegato (interno e/o esterno). E' possibile aggiungere allegati non ufficiali.	Documento	No	No
Tab Annotazioni	Riporta informazioni e note dell'utente utili a fini di protocollo, di archiviazione e di trattamento dell'atto	Testo	No	No
Tab Visibilità	Indica la visibilità definita per la scheda documentale	Lista	Sì	Sì

Il RSP, 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 RSP, 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'Istituto.

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. In ogni caso, in sede di trasmissione al sistema di conservazione le relative schede documentali sono immodificabili.

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.

In allegato (Allegato 3 – Casi particolari della registrazione di protocollo) è prevista una modalità operativa per i casi eccezionali di differimento dell'associazione della registrazione ai relativi documenti.

5.4. Livello di riservatezza

Qualora l'addetto alla protocollazione valuti il documento come non riservato, imposta lo stesso come L2, indicandolo nell'apposito campo.
Qualora, invece, il documento sia valutato di natura riservata di livello 4, l'addetto alla protocollazione gli assegna la conseguente classificazione e procede come indicato nella regolamentazione interna sulla riservatezza.

È possibile impostare il profilo di riservatezza del documento. Al momento il sistema prevede cinque livelli di riservatezza così definiti:

- livello 0: pubblico (relativo a documenti esportabili su internet);
- livello 1: a diffusione interna (relativo a documenti esportabili su intranet CONSOB);
- livello 2: non riservato (relativo a documenti di tipo istruttorio);
- livello 3: riservato (relativo a documenti il cui procedimento è riservato);
- livello 4: segreto (relativo a documenti di massima riservatezza, i cosiddetti L4).

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 DEMACO 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:

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

Per i documenti informatici in partenza, in particolare, la segnatura viene apposta mediante una firma elettronica, generata automaticamente dal sistema informatico, con indicazione nel certificato del codice identificativo dell'Istituto.

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:

- codice identificativo dell'Istituto;
- 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 il Protocollo in ordine di numero di protocollo.

La segnatura è realizzata con una etichetta autoadesiva corredata di codice a barre (cfr. A9 – Loghi, timbri, etichette CONSOB), 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 comporta l'obbligo di annullare l'intera registrazione di protocollo.
La funzione di annullamento delle registrazioni di protocollo è accessibile solo al RSP, ai suoi delegati e agli addetti al Protocollo, 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 RSP, o delegati, con un messaggio in DEMACO 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 RSP, 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.

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 RSP o suoi delegati, qualora per cause tecniche non sia possibile utilizzare la procedura informatica DEMACO 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 Segreterie di UO, provvedono a registrare in DEMACO, 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 DEMACO e dislocato presso le strutture di Protocollo nelle due sedi di Roma e Milano (Allegato 7 – Piattaforma DEMACO.).

5.8. Documenti esclusi dalla protocollazione e casi particolari di registrazione

La casistica d'Istituto dei documenti esclusi dalla protocollazione e dei casi particolari di registrazione di protocollo sono descritti in A8 – Elenco dei documenti esclusi dalla registrazione di protocollo.

5.9. Gestione delle registrazioni di protocollo tramite DEMACO

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 DEMACO.
Il sistema di sicurezza adottato dall'Istituto 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 DEMACO 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'Istituto 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;
- applicazione della firma digitale al file così realizzato;
- 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 su supporti rimuovibili non riscrivibili.
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 delle copie del registro informatico di protocollo

È compito del responsabile della conservazione dei documenti, o suoi delegati, provvedere alla verifica del contenuto dei supporti prodotti dal sistema e alle operazioni relative al trasferimento su supporto separato del registro di protocollo.
Un duplicato del registro di protocollo può essere, altresì, conservato dal RSP, o suoi delegati, mentre il supporto generato dal sistema è gestito nel sistema di conservazione.
Le modalità di gestione di tali supporti sono definite dal RSP dell'Istituto, o suoi delegati, secondo quanto disposto nel presente Manuale.
I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.

5.11. Descrizione funzionale ed operativa del sistema di protocollo informatico

La descrizione funzionale ed operativa del sistema di dematerializzazione DEMACO, incluso il sistema di protocollo informatico e di gestione dei flussi documentali, è parte del manuale utente (Allegato 6 – Piattaforma DEMACO. Manuale utente).

6. Registri di archivio

Per "Registro di archivio" si intende una specifica partizione del sistema documentale dedicata ad una serie di tipologie documentali.

Nella tabella seguente è riportata la lista dei Registri gestiti in DEMACO finalizzata all'archiviazione dei documenti dell'Istituto.

Alcuni dei registri sono soggetti non solo alla registrazione di protocollo ma anche a registrazione particolare da parte dell'Istituto; sono associati ad un numero identificativo univoco i registri di: Delibere, Disposizioni, Ordini di Servizio, Verbali e di Lavoro[12].
Ad ogni tipo documento del registro di "Predisposizione" è associato un processo automatico che ne consente l'archiviazione nel relativo Registro.

Non sono ammessi documenti che rimangano allo stato di "predisposizione": tutti i documenti in "predisposizione" devono essere consolidati e archiviati negli appositi registri previsti, salvo i casi previsti dal presente Manuale (ad esempio i casi di documenti in attesa di approvazione e/o firma). Il registro di "Predisposizione" è finalizzato alla preparazione e formazione della bozza di un documento che sarà poi consolidato, registrato e archiviato in forma ufficiale. I documenti che non necessitano di archiviazione ufficiale sono inseriti nell'apposito Registro di lavoro.

Identificativo Registro	**Tipo documento**	**Descrizione**
Predisposizione	Comunicazioni in uscita Comunicazioni interne Delibere Disposizioni OdS Verbali	Archivio per la predisposizione dei documenti dell'Istituto
Protocollo Ufficiale	Protocollo in ingresso Protocollo in uscita	Protocollo dell'Istituto
Registro Giornaliero	Scheda Registrazioni	Registro giornaliero di protocollo
Registro Delibere	Delibere Ufficiali	Archivio delle Delibere
Registro Disposizioni	Disposizioni Ufficiali	Archivio delle Disposizioni
Registro Ordini di Servizio	Ordini di Servizio Ufficiali	Archivio degli OdS
Registro Verbali	Verbali Ufficiali	Archivio dei verbali
Registro di Lavoro	Documenti di Lavoro	Archivio delle "carte di lavoro"

Tutta la documentazione che nel corso di un'istruttoria non richiede protocollazione ma che è utile/necessario inserire nel fascicolo istruttorio può essere acquisita digitalmente e archiviata all'interno del "Registro di Lavoro" (ivi inclusi gli archivi di e-mail o singole e-mail), procedendo anche alla relativa classificazione nonché all'inserimento nei fascicoli di riferimento.
Lo stesso vale per i documenti annotati a penna e per qualsiasi tipologia di documento che possa essere utile conservare nei fascicoli presenti nell'archivio d'Istituto: in tal caso sono scansionati e inseriti nel Registro di lavoro.

Con l'esclusione dei Registri e dei tipi di documenti inerenti alla protocollazione trattati in precedenza (cfr. capitolo 5), per quanto concerne la documentazione ufficiale è previsto un

[12] A questi si aggiungono: il registro riservato del Presidente, finalizzato alle comunicazioni riservate da parte del Presidente, gestito su supporto cartaceo; il registro della Camera di Conciliazione e Arbitrato, per le comunicazioni degli atti da parte dell'organismo, gestito con un apposito applicativo software gestionale.

archivio per ciascuna tipologia documentale, mentre nell'archivio di "Predisposizione" sono previste ulteriori quattro tipologie documentali.
Le schede associate alle tipologie documentali sono caratterizzate principalmente da una serie di metadati, da un documento principale, da uno o più allegati, dal mittente o destinatario del documento.

6.1. Documenti soggetti a registrazione particolare

Di seguito si descrive, ai sensi delle "Regole tecniche sul protocollo informatico", l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui essi si riferiscono.
Questo tipo di registrazione consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti; nello specifico, la classificazione, la fascicolazione, l'archiviazione, nonché la successiva protocollazione nel caso di invio all'esterno del documento, attraverso l'utilizzo di una nota di accompagnamento. Le Delibere ufficiali, in particolare, possono essere pubblicate sul sito internet istituzionale, attraverso l'utilizzo di un apposito software dedicato a tale gestione.

Tali documenti costituiscono delle serie di interesse archivistico, ciascuna delle quali è corredata di un repertorio contenente le seguenti informazioni:

- dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, data di adozione, oggetto,…);
- numero progressivo (di repertorio);
- dati di classificazione e di fascicolazione.

6.2. Formati e metadati delle tipologie di documenti informatici

6.2.1. Registro di "Predisposizione"

Per la tipologia documentale "Delibere" sono stati individuati i seguenti metadati:

Metadati "Delibere"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Progressivo	Numero assegnato in automatico al documento in predisposizione	Testo	Automatico	Sì
Data Documento	Data assegnata in automatico al documento in predisposizione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Data Proposta di Commissione	Data di proposta della deliberazione	Data	Sì	Sì
Tipo Firma	Firma digitale	Lista	No	Sì
Da Modificare	Indica la deliberazione con modifiche (Si, No)	Lista	Sì	Sì
Stato	Campo di sistema che indica lo stato del processo di archiviazione della scheda di predisposizione (In predisposizione, Archiviato)	Testo	Automatico	Sì
Modello	Modello del documento in predisposizione (Delibera)	Lista	Alfanumerico	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

Per la tipologia documentale “Disposizioni” sono stati individuati i seguenti metadati:

Metadati “Disposizioni”				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Progressivo	Numero assegnato in automatico al documento in predisposizione	Testo	Automatico	Sì
Data Documento	Data assegnata in automatico al documento in predisposizione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d’Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell’atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale, Firma digitale (senza invio PEC)	Lista	No	Sì
Stato	Campo di sistema che indica lo stato del processo di archiviazione della scheda di predisposizione (In predisposizione, Archiviato)	Testo	Automatico	Sì
Modello	Modello del documento in predisposizione (Disposizione)	Lista	Alfanumerico	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

Per la tipologia documentale “OdS” sono stati individuati i seguenti metadati:

Metadati “OdS”				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Progressivo	Numero assegnato in automatico al documento in predisposizione	Testo	Automatico	Sì
Data Documento	Data assegnata in automatico al documento in predisposizione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d’Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell’atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale	Lista	No	Sì
Stato	Campo di sistema che indica lo stato del processo di archiviazione della scheda di predisposizione (In predisposizione, Archiviato)	Testo	Automatico	Sì
Modello	Modello del documento in predisposizione (OdS)	Lista	Alfanumerico	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

Per la tipologia documentale “Verbali” sono stati individuati i seguenti metadati:

Metadati “Verbali”				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Progressivo	Numero assegnato in automatico al documento in predisposizione	Testo	Automatico	Sì
Data Documento	Data assegnata in automatico al documento in predisposizione	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d’Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell’atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale	Lista	No	Sì
Stato	Campo di sistema che indica lo stato del processo di archiviazione della scheda di predisposizione (In predisposizione, Archiviato)	Testo	Automatico	Sì
Modello	Modello del documento in predisposizione (Verbale)	Lista	Alfanumerico	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.2. Archivio "Registro Delibere"

Per la tipologia documentale "Delibere Ufficiali" sono stati individuati i seguenti metadati:

Metadati "Delibere Ufficiali"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Identificativo di Sistema	Numero assegnato in automatico al documento	Testo	Automatico	Sì
Data Archiviazione	Data assegnata in automatico al documento	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Numero Delibera	Identificativo univoco della delibera sequenziale negli anni.	Alfanumerico	Automatico	Sì
Data Delibera	Data della delibera	Data	No	Sì
Tipo Firma	Firma digitale, Firma autografa (Presidente_DG)	Lista	No	Sì
Estensione Numero Delibera	Estensione eventualmente correlata ad un numero di delibera (es. BIS)	Alfanumerico	No	No
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.3. Archivio "Registro Disposizioni"

Per la tipologia documentale "Disposizioni Ufficiali" sono stati individuati i seguenti metadati:

Metadati "Disposizioni Ufficiali"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Disposizione	Numero assegnato in automatico al documento	Testo	Automatico	Sì
Data Archiviazione	Data assegnata in automatico al documento	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale, Firma autografa (Presidente_DG)	Lista	No	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.4. Archivio "Registro Ordini di servizio"

Per la tipologia documentale "OdS Ufficiali" di servizio sono stati individuati i seguenti metadati:

Metadati "OdS Ufficiali"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero OdS	Numero assegnato in automatico al documento	Testo	Automatico	Sì
Data Archiviazione	Data assegnata in automatico al documento	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale	Lista	No	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.5. Archivio "Registro Verbali"

Per la tipologia documentale "Verbali Ufficiali" sono stati individuati i seguenti metadati:

Metadati "Verbali Ufficiali"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Verbale	Numero assegnato in automatico al documento	Testo	Automatico	Sì
Data archiviazione	Data assegnata in automatico al documento	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	No	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Tipo Firma	Firma digitale	Lista	No	Sì
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.6. Archivio "Registro di Lavoro"

Per la tipologia documentale "Documenti di Lavoro" sono stati individuati i seguenti metadati e non è prevista una fase di predisposizione e relativo processo automatico di archiviazione.

Metadati "Documenti di Lavoro"				
Nome dato	**Descrizione**	**Tipo**	**Modificabile**	**Obbligatorio**
Numero Documento	Numero assegnato in automatico al documento	Testo	Automatico	Sì
Data inserimento	Data assegnata in automatico al documento	Data	Automatico	Sì
Titolo / Classe	Classificazione in base al Titolario d'Istituto	Lista	Sì	Sì
Livello riservatezza	Definizione livello di riservatezza dell'atto documentale	Testo (L0-L4)	No	Sì
Data scadenza riservatezza	Data di scadenza del livello di riservatezza, preimpostata dal sistema. Non obbligatorio per L0-L1.	Data	No	No
Data documento	Data del documento	Data	Sì	No
Tipo Comunicazione	Comunicazione per l'esterno o per l'interno	Testo	Sì	Sì
Diffusione interna	Indica se il documento è a diffusione interna (quale CaP: Comunicazioni al Personale)	Testo (flag SI/NO)	Sì	Sì
Data Protocollo del documento	Data relativa al protocollo del documento inserito	Data	Sì	No
Vettore in assenza PEC	Vettore della comunicazione in assenza di PEC	Lista	Sì	Sì
Numero Sird	Eventuale riferimento a pratiche, presenti nel sistema interno Sird, relative al documento registrato	Testo	Sì	No
Oggetto	Oggetto del documento secondo gli standard definiti	Testo	No	Sì

6.2.7. Numerazione dei registri di archivio

La numerazione delle registrazioni è legata all'archivio utilizzato; per quanto concerne la gestione della documentazione "Delibere ufficiali", "Disposizioni ufficiali", "OdS Ufficiali" e "Verbali Ufficiali" sono creati altrettanti Registri, che gestiscono l'identificazione della scheda con una numerazione sequenziale (Delibere) e su base annua (Disposizioni, Ods e Verbali).

La numerazione sequenziale è gestita in automatico dalla piattaforma DEMACO attraverso l'uso di un campo dedicato: ciò comporta che il nuovo riferimento è presente come campo ricercabile nella scheda documentale insieme al campo "numero progressivo" che è usato, invece, come dato identificativo di sistema.
La numerazione su base annua è composta da sette cifre numeriche più due dell'anno di esercizio. A tal riguardo l'archivio di "Predisposizione", presente in DEMACO, è integrato con altre quattro tipologie documentali: "Delibere", "Disposizioni ", "OdS" e "Verbali". Queste seguono la numerazione su base annuale usata nelle altre tipologie documentali contenute nell'archivio.

7. Sistema di gestione archivistica

7.1. Generalità

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

Con specifico riferimento alla documentazione analogica, le linee guida presenti in A1 – Linee guida per gli archivi di deposito e storico, illustrano principi e procedure da seguire per la corretta formazione e gestione degli archivi di deposito e storico.

7.2. Misure di tutela e valorizzazione dell'archivio dell'Istituto

La CONSOB, in quanto ente con personalità giuridica di diritto pubblico munito di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, non è soggetta alle disposizioni in vigore per la amministrazioni statali per quanto attiene alla tenuta degli archivi e allo scarto.
La documentazione prodotta da CONSOB 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 di CONSOB di ordinare e inventariare i propri archivi storici rendendoli accessibili alla consultazione.

L'archivio e i singoli documenti dell'Istituto 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'Istituto, 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'Istituto 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.

7.3. Titolario dell'Istituto

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'Istituto, al quale deve ricondursi la molteplicità dei documenti prodotti, per organizzarne l'ordinata sedimentazione.

Il Titolario d'Istituto 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 in A10 – Titolario di Classificazione .

Per ciascun livello è previsto il relativo "Indice di classificazione", cioè il valore numerico che lo identifica in maniera univoca. Il Titolario d'Istituto adotta una numerazione mediante cifre indo-arabiche separate dal punto.

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

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

L'approvazione e le modifiche del Titolario sono di competenza della Commissione.

7.4. 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'Istituto; 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 titolario è uno strumento di gestione documentale onnicomprensivo, finalizzato a prevedere e organizzare quanto l'Istituto pone e porrà in essere sul piano documentale nell'ambito delle funzioni sue proprie.

Tutti i documenti ricevuti e prodotti dalle UO dell'Istituto, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al Titolario.
Mediante la classificazione si assegna al documento l'indice di classificazione costituto da titolo e classe.
L'Istituto 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 titolario, 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'Istituto alla data di approvazione del titolario.
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.

7.5. 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 DEMACO 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.

7.6. Piano di fascicolazione

La mappatura delle tipologie di fascicoli previste dall'Istituto, 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 4 – 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 RSP 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'Istituto.

7.7. 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'Istituto sono state previste quattro tipologie di fascicolo:

1. Fascicolo "Procedimento 241"
2. Fascicolo "Istruttorio"
3. Fascicolo di "Attività"
4. Fascicolo di "Persona fisica o giuridica".

7.7.1. 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. In Allegato (Allegato 4 – Piano di Classificazione e Fascicolazione archivistica) è riportata la Tabella dei procedimenti 241 dell'Istituto, con l'indicazione della classifica d'archivio e della denominazione standard prevista.

Tali fascicoli si aprono al livello più basso del titolario 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'Istituto:
- il fascicolo del Piano strategico;
- il fascicolo di vigilanza;
- il fascicolo giudiziario;
- il fascicolo di attività sanzionatoria.

7.7.2. 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.

7.7.3. Fascicolo di "persona fisica o giuridica"

Indica il fascicolo di 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 d'Istituto, 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'Istituto. 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 nel titolo *10. Gestione del personale* ed è il caso consigliato in dottrina e in pratica) e a livello di classe (plausibile secondo le esigenze organizzative dell'Istituto).

Quanto osservato vale, con le differenze del caso, anche per il fascicolo per "soggetto giuridico" (ad es. emittente quotato, promotore finanziario, etc.), nel quale si andranno a raccogliere i documenti propri che attengono a quel determinato soggetto.
A tale proposito, per l'Istituto, è previsto l'utilizzo di fascicoli di tal tipo per la raccolta dei documenti connessi ad attività di "vigilanza continuativa".

7.7.4. 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.

7.7.5. Profili gestionali dei fascicoli: autonomi, condivisi, pubblici

A prescindere dalle tipologie di fascicolo sopra enunciate, nell'Istituto si prevedono tre profili principali di gestione.

- *Fascicolo autonomo*. La condivisione operativa fra l'UO master e altre UO è minima o nulla. La visibilità del fascicolo è con autorizzazione. Si tratta di fascicoli di assoluta ed esclusiva pertinenza e competenza di una sola UO per i quali non si prevede, se non in casi eccezionali, il coinvolgimento di altre UO nella loro alimentazione.
- *Fascicolo condiviso*. La condivisione operativa fra l'UO master e altre UO è ampia. La visibilità del fascicolo è con autorizzazione. Si tratta di fascicoli utilizzati da più UO per finalità gestionali, delle quali una UO è master. Riguarda, in genere, fascicoli che nascono per gestire documentazione relativa ad attività trasversali o di supporto dell'Istituto: quelle che interessano, in particolare, l'area amministrativa, la contabilità, la pianificazione, il personale, etc. Nel Piano di fascicolazione si danno indicazioni circa i fascicoli da creare e la UO di riferimento.
- *Fascicolo pubblico*. La condivisione operativa tra la UO master e le altre UO è massima. La visibilità del fascicolo è completa. Esempi di questo tipo sono: i fascicoli per i documenti alla firma del Presidente o del DG; i fascicoli per l'Ordine del Giorno della Commissione.

Questi profili non sono selezionabili funzionalmente in Demaco, ma è obbligatorio fare riferimento a essi quando si crea e si gestisce un fascicolo. Uno dei motivi principali consiste nel facilitare la condivisione di informazioni, prevedendo la visibilità di quei fascicoli ai quali si riconosce un preminente carattere strutturale di condivisione se non di pubblicità.
L'esempio classico concerne i fascicoli relativi alle attività cosiddette trasversali o di supporto per il personale dell'Istituto e, più in generale, quelle di carattere amministrativo, per lo svolgimento delle quali è implicita in molti casi la collaborazione funzionale tra più utenti. In altri termini: è errato creare fascicoli relativi ad attività di tipo gestionale solo per fascicolare la semplice e unica risposta ad una richiesta da parte di una UO, con duplicazione del fascicolo e ridondanza

informativa. È necessario che, in questi casi, la UO master estenda la visibilità del fascicolo alle UO coinvolte nell'attività per consentirvi l'inserimento diretto della risposta (cosa che peraltro avverrà in ogni caso, ma a cura della UO master).

In generale, una volta aperto un fascicolo in base ai profili sopra riportati, tutte le UO che ricevono o producono documenti attinenti allo specifico procedimento o attività devono obbligatoriamente inserirli in quello stesso fascicolo, anche se aperto da altra UO, che avrà cura di estenderne la visibilità per competenza.

Si rammenta, in tal senso, che DEMACO prevede un meccanismo di visibilità incrociata tra fascicolo e documento; è possibile dare la visibilità di un fascicolo ma non quella dei documenti in esso contenuti e viceversa.

È possibile, inoltre, definire il profilo di riservatezza prevalente del fascicolo. Al momento il sistema prevede cinque livelli di riservatezza così definiti:

- livello 0: pubblico (con documenti esportabili su internet);
- livello 1: a diffusione interna (con documenti esportabili su intranet CONSOB);
- livello 2: non riservato (con documenti di tipo istruttorio);
- livello 3: riservato (con documenti il cui procedimento è riservato);
- livello 4: segreto (con documenti di massima riservatezza, i cosiddetti L4).

7.8. 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 funzionario 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.

Dato	Descrizione	Tipo	Modificabile	Obbligatorio
- Metadati identificativi				
Id Fascicolo	Identificativo univoco del fascicolo all'interno del sistema	Numerico	Automatico	Sì
Anno	Anno di riferimento del fascicolo	Numerico	Automatico	Sì
Progressivo	Numero sequenziale progressivo nell'ambito della classificazione e dell'anno del fascicolo	Numerico	Automatico	Sì
Classificazione	Classificazione in base al Titolario d'Istituto	Lista	Sì	Sì
- Metadati descrittivi				
Data apertura	Data di apertura del fascicolo, preimpostata da sistema con la data odierna	Data	Sì	Sì
Data chiusura	Data di chiusura del fascicolo	Data	Sì	No
Data scadenza	Data di scadenza eventualmente pianificata per il fascicolo. Dato obbligatorio nel caso di tipo fascicolo relativo a Procedimento 241	Data	Sì	No
Creato da	Nome utente creatore del fascicolo	Testo	Automatico	Sì
Modificato da	Nome utente dell'eventuale modifica	Testo	Automatico	Sì
Oggetto	Oggetto del fascicolo in base agli standard definiti	Testo	Sì	Sì
Soggetti	Identificativo e denominazione dei soggetti interessati o coinvolti nel fascicolo	Testo	Sì	No

- Metadati relazionali				
Stato	Stato di lavorazione del fascicolo (aperto, chiuso, sospeso, interrotto)	Lista	Sì	Sì
Posizione d'archivio	Posizione di gestione archivistica del fascicolo (Corrente/Deposito/Storico)	Lista	Sì	Sì
Tipo Fascicolo	Tipologia del fascicolo (241, istruttorio, attività, persona)	Lista	Sì	Sì
Livello riservatezza	Livello di riservatezza dei documenti in prevalenza presenti nel fascicolo (L0-L4)	Lista	Sì	No
Id Operazione	Identificativo operazione in caso di richiamo manuale al numero di un altro fascicolo	Testo	Sì	No
Id Pratica	Identificativo pratica in caso di fascicolo ibrido	Testo	Sì	No
- Metadati amministrativi				
Responsabile	Nome utente responsabile del fascicolo. Dato obbligatorio in caso di procedimento 241	Lista	Sì	No
Assegnatario	Nome utente assegnatario del fascicolo.	Lista	Sì	No
Divisione/UNC	Divisione titolare del fascicolo	Testo	Automatico	Sì
Ufficio	Ufficio titolare del fascicolo	Testo	Automatico	No
Procedimenti	Denominazione del procedimento associato al fascicolo	Lista	Sì	No
Autorizzazioni Selezione	Seleziona la visibilità dei metadati di copertina del fascicolo: non implica la visibilità dei relativi documenti inseriti nel fascicolo	Lista	Sì	No
Visibilità completa	Seleziona la visibilità a tutti gli utenti della copertina (cd. Fascicolo pubblico)	Flag	Sì	No
Storia	Visualizza il tracciamento della storia delle operazioni effettuate sul fascicolo	Lista	No	Automatico
- Metadati gestionali				
Collega fascicoli	Funzione di collegamento informativo con altri fascicoli del sistema; riporta la descrizione del collegamento, l'oggetto del fascicolo collegato e l'eventuale Id Operazione.	Testo	Sì	No

Le informazioni indicate compaiono nella maschera del fascicolo informatico (Allegato 6 – Piattaforma DEMACO. Manuale utente).

Il fascicolo è aperto al secondo livello del Titolario (classe).

Il fascicolo è caratterizzato dai seguenti elementi distintivi:

a. anno di istruzione;
b. indice di classificazione;
c. numero progressivo nell'ambito della classificazione;
d. oggetto.

Di norma per l'identificazione univoca del fascicolo è adottato nelle comunicazioni il valore presente nel campo "Id Fascicolo", che è correlato agli elementi distintivi sopra illustrati.

Oltre agli elementi classificatori e all'oggetto, concorrono all'identificazione del fascicolo alcuni elementi gestionali, quali l'indicazione dell'unità organizzativa titolare del fascicolo e del RdP.

7.9. 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 noma, 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.
Perché il sistema di gestione documentale fondato sulla fascicolazione sia efficiente è, infine, necessario procedere nel senso di una normalizzazione della descrizione dell'oggetto del fascicolo. Specifiche raccomandazioni in tal senso, basate su standard nazionali e internazionali, sono indicate in allegato (Allegato 4 – Piano di Classificazione e Fascicolazione archivistica).

7.10. Assegnazione del fascicolo

Il sistema prevede, con apposita funzionalità, di assegnare un fascicolo ad uno o più utenti, con sola visibilità o con assegnazione lavorazione.

In particolare in caso di assegnazione dei fascicoli relativi a procedimenti amministrativi, questa attività corrisponde ad una formale assegnazione per lo svolgimento delle attività del procedimento stesso.

In ogni caso l'assegnazione del fascicolo può avvenire con o senza l'estensione della visibilità in competenza dei relativi documenti.

7.11. Il sottofascicolo

Il fascicolo può essere suddiviso in sottofascicoli. Queste suddivisioni sono identificate con un'ulteriore catena numerica, che si riferisce gerarchicamente al numero di fascicolo dal quale è separata da un punto.
Il sottofascicolo eredita le seguenti informazioni dal fascicolo in cui è aperto:

- l'anno di apertura;
- l'indice di classificazione;
- il numero progressivo nell'ambito della classificazione;
- la visibilità (utenti e UO).

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

7.12. 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.
Il fascicolo chiuso è di norma gestito secondo i principi di archivio di deposito e storico riportati in A1 – Linee guida per gli archivi di deposito e storico.

7.13. Gestione dei fascicoli "ibridi"

I fascicoli relativi ad attività istruttorie già avviate alla data del 1° luglio 2013, ovverosia prima dell'avvio dell'operatività del sistema DEMACO, hanno una composizione "ibrida", vale a dire sono costituiti da documenti in parte cartacei ed in parte digitali. La loro gestione è disciplinata come di seguito indicato.

Sui documenti da trasmettere all'esterno relativi ad istruttorie con fascicolo "ibrido" è necessario riportare sia il precedente numero di procedimento che il nuovo numero di fascicolo DEMACO che deve essere creato per aggregare i documenti digitali.

L'utente ha cura di indicare:

- sulla copertina del fascicolo cartaceo, oltre al numero di procedimento precedentemente assegnato, il numero del fascicolo DEMACO;
- sul fascicolo elettronico nel campo "Id pratica", il numero di procedimento precedentemente assegnato e indicato sulla copertina del fascicolo cartaceo.

Alla conclusione dei procedimenti e delle attività cui si riferiscono, i fascicoli vanno trasmessi all'archivio di deposito a cura delle UO di competenza, a seguito dell'acquisizione via scanner dei documenti ivi contenuti e del loro inserimento nel fascicolo DEMACO riferito allo stesso procedimento. Con la trasmissione del fascicolo cartaceo all'archivio di deposito si procede contestualmente alla chiusura del fascicolo DEMACO.

8. Sistema di conservazione digitale dei documenti

8.1. Principi generali

La conservazione dei documenti digitali a norma prevede il rispetto dei principi di seguito richiamati.

La definizione e messa in esercizio di un sistema di conservazione unico che assicuri, dalla presa in carico fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie dei seguenti oggetti, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) i fascicoli informatici ovvero le aggregazioni documentali informatiche (quali ad esempio i Registri di archivio) con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Con specifico riferimento alla gestione dei documenti, il sistema di conservazione assicura:

a) l'identificazione certa della CONSOB e del soggetto che ha formato il documento, cioè la sua autenticità;
b) l'integrità del documento e la sua affidabilità nel tempo;
c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative connesse, inclusi i dati di registrazione e di classificazione;
d) il rispetto delle misure di sicurezza previste dalle vigenti normative in materia di tutela dei dati personali (privacy).

Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione, dal versamento allo scarto, dell'oggetto conservato (documento, fascicolo) nell'ambito del processo di conservazione, promuovendo una convergenza funzionale da eventuali diversi canali di versamento (principio di centralità di archivio).
Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla normativa di riferimento, indipendentemente dall'evolversi del contesto tecnologico.
Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi (o lotti) che si distinguono in:

a) *pacchetti di versamento*, cioè i pacchetti informativi inviati dal produttore al sistema di conservazione secondo un formato predefinito e descritto nel relativo manuale;
b) *pacchetti di archiviazione*, cioè i pacchetti informativi composti dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche regole tecniche sulla conservazione e secondo le modalità riportate nel relativo manuale;
c) *pacchetti di distribuzione*, cioè i pacchetti informativi inviati dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Il sistema di conservazione opera secondo modelli organizzativi definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale. In ambito CONSOB, ai sensi della normativa vigente, il RSP, o suoi delegati, ricopre anche il ruolo di Responsabile della conservazione e si avvale di delegati preposti alle funzioni di gestione documentale e degli archivi e alla conservazione indicate nel capitolo 1. I delegati operano in coordinamento e come sostituti reciproci in caso di assenza o impedimento dell'uno o dell'altro.

8.2. Modello di funzionamento

I documenti e i fascicoli sono conservati, anche sulla base delle tempistiche previste dalla normativa di riferimento, nel sistema di conservazione secondo precise regole operative, su supporti elettronici certificati dal responsabile della conservazione. Ogni oggetto conservato è tenuto costantemente sotto controllo dal sistema, che ne garantisce la leggibilità e la disponibilità per un periodo prestabilito in fase di configurazione.
Gli oggetti sono conservati su supporti digitali sulla base dei seguenti criteri di catalogazione: Istituto, Registro, Tipo documento.
La CONSOB rappresenta l'Area Organizzativa Omogenea di riferimento, il Registro rappresenta la macrocategoria dei documenti, mentre il Tipo documento consente di suddividere i documenti all'interno di uno specifico Registro. A ogni Registro/Tipo documento vengono associate le informazioni sulle modalità e sui tempi di conservazione dei documenti.

Il processo di conservazione è realizzato attraverso un flusso di lavorazione degli oggetti, a ciascuno dei quali viene associato uno stato di lavorazione che indica in ogni istante in quale fase del processo si trova.
Il flusso può essere automatizzato; l'unico stato di lavorazione nel quale è necessario l'intervento manuale è quello della certificazione del supporto, per il quale è richiesta l'apposizione della firma digitale del responsabile della conservazione o suoi delegati.

Nella prima fase del processo i documenti vengono immessi nel sistema di conservazione attraverso meccanismi automatici di trasferimento. I documenti sono controllati e raccolti per tipologie documentali in un supporto prodotto in base a specifiche regole di raggruppamento (dimensioni massime, numero documenti, etc.). All'interno del supporto viene inserito un documento di riepilogo di tutti i documenti.

Il processo di conservazione dei documenti termina con l'apposizione da parte del conservatore della firma digitale e della marca temporale quali strumenti di "certificazione" opponibile a terzi sull'insieme di documenti destinati alla conservazione e su un'evidenza informatica (file di chiusura) contenente i metadati e le impronte (hash) dei documenti stessi. Il file di chiusura generato dal sistema risponde ai canoni dello standard UNI 11386:2010 (SInCRO).
È, infatti, la tecnologia della firma digitale che permette di garantire l'autenticità e di rendere immodificabile un oggetto informatico. La firma associata alla marcatura temporale permette di datare in modo certo l'oggetto conservato.
Per i documenti informatici generati da "documenti analogici originali unici" è prevista l'apposizione del riferimento temporale e della firma digitale da parte del responsabile della conservazione, anche in qualità di pubblico ufficiale. Quest'ultimo adempimento è finalizzato ad attestare la conformità della procedura di riproduzione in formato digitale del documento analogico d'origine effettuata in sede di acquisizione e archiviazione.

La conservazione di documenti nel sistema è riassumibile nelle seguenti fasi di processo:
1. definizione delle regole di conservazione che il documento deve osservare: generalmente dipendono dalla tipologia documentale a cui è associato;
2. verifica delle regole di conservazione ed esecuzione delle operazioni necessarie (firma, marca) in base alla tipologia documentale di appartenenza del documento;
3. acquisizione (intesa come versamento) del documento nel sistema;

4. verifica automatica delle scadenze e dell'integrità dei documenti;
5. archiviazione del documento in un pacchetto digitale (creazione del cd. "supporto" virtuale);
6. certificazione del supporto virtuale in base al modello associato alla tipologia documentale;
7. creazione delle copie del supporto virtuale (copie automatiche di backup);
8. verifica delle scadenze e dell'integrità dei supporti e del loro contenuto.

Il processo di conservazione è basato sulla tipologia documentale: ad essa si collegano tutti i modelli necessari all'esecuzione delle operazioni automatiche o manuali.

8.3. Descrizione del sistema

Nella presente sezione sono illustrate le componenti tecnologiche, fisiche e logiche del sistema di gestione e di conservazione DEMACO e le relative procedure di gestione.

8.3.1. Architettura generale

L'architettura del sistema è strutturata in modo tale da suddividere la parte di presentazione web dalla parte applicativa. Tale configurazione architetturale permette di creare una netta separazione tra i moduli d'interazione con l'utente (i.e. interfacce web) e i sistemi contenenti la *business logic* e la comunicazione con la base dati.

L'architettura è realizzata, quindi, secondo il seguente schema logico:

- *Presentation Layer*: fornisce l'accesso via web alle operazioni del responsabile della conservazione e permette di certificare i supporti da conservare;
- *Application Layer*: fornisce i servizi per accedere ai dati ed ai documenti posti in conservazione e tutti i servizi necessari per eseguire la conservazione secondo la normativa in vigore;
- *Data Layer* (DBMS): contiene tutte le informazioni di configurazione dell'applicativo ed i metadati dei documenti conservati all'interno del database;
- *Client*: permette di utilizzare il sistema in tutte le sue peculiarità, per quanto concerne l'amministrazione e i moduli del prodotto;
- *Web client*: permette di accedere ai moduli del sistema di conservazione attraverso l'applicazione web;
- *Storage*: contiene il volume dei pacchetti di conservazione, ovvero i "supporti/documenti" e i "supporti di materializzazione";
- *Back-up*: contiene le copie di backup previste dalla legge (minimo due) all'interno di *file system* dedicati[13].

Il *Presentation Layer* è costituito da più server di *front-end* e utilizza tecnologie che gestiscono e bilanciano il traffico da parte dei client preposti alla gestione della conservazione sostitutiva.

L'*Application Layer* è costituito da più server di *back-end* configurati in modalità *cluster*.

Il *Data Layer* per la base dei dati di conservazione è costituito dal database in modalità *cluster* che supporta le caratteristiche di ricerca standard.

[13] Nell'ambito delle procedure di sicurezza si prevede una copia di ridondanza dei dati nelle due sedi di Roma e Milano.

I supporti/documenti "in linea" (cioè il volume di sistema) è costituito da uno spazio fisico senza particolari requisiti software, ma tale da poter essere raggiunto attraverso una condivisione di rete ai server dell'*Application Layer*.

Il supporti di "materializzazione" hanno le stesse caratteristiche definite per i supporti/documenti "in linea", ma prevede almeno due siti fisici diversi su cui salvare le "copie" previste dalla normativa.

8.3.2. Caratteristiche funzionali

Il *Presentation Layer* è costituito da un'applicazione web installata sul server web e raggiungibile attraverso il browser.

L'*Application Layer* contiene i servizi informatici che permettono di eseguire gli steps definiti per la conservazione:

- *Accettazione*: permette di prelevare i documenti attraverso l'utilizzo del componente software presente sul server;
- *Creazione Supporti*: permette di creare il file contenente le impronte dei documenti da conservare;
- *Certificazione Supporti*: permette, successivamente alla firma, di apporre il riferimento temporale sui supporti;
- *Materializzazione Supporti*: permette di creare le copie di backup previste dalla normativa;
- *Monitoraggio Completo*: permette di monitorare lo stato dell'archivio e di verificare la validità dei documenti/supporti presenti;
- *Entity Server*: permette di gestire le immagini in modalità client/server.

8.4. Tipologie degli oggetti sottoposti a conservazione

8.4.1. Registro "Protocollo Ufficiale" e "Registro Giornaliero" di protocollo

I documenti informatici archiviati nel registro di "Protocollo Ufficiale" sono trasferiti giornalmente nel sistema di conservazione sostitutiva con un processo automatico che provvede al trasferimento dei seguenti documenti:

- Documenti protocollati fino alla data odierna e non ancora posti in conservazione che siano correttamente classificati, fascicolati e che contengano il documento principale;
- Registro giornaliero di protocollo, generato a cadenza giornaliera e firmato dal RSP, o suoi delegati.

Al fine di gestire le suddette tipologie nel sistema di conservazione sono definiti i tipi documento: "Protocollo Ufficiale" e "Registro giornaliero".
Il tipo documento relativo al registro di "Protocollo Ufficiale" consente di gestire i flussi giornalieri dei documenti protocollati; per ognuno di essi sono registrate le seguenti informazioni: estremi di protocollo (numero e data protocollo), oggetto e classificazione.
Il tipo "Registro giornaliero" consente di gestire in conservazione il registro di protocollo del sistema. Ogni giorno il sistema fornisce un documento riassuntivo dei protocolli assegnati riportante almeno i seguenti dati:

- Progressivo;
- Data registrazione;
- Oggetto.

Il processo automatico di trasferimento nel sistema di conservazione si realizza con le seguenti fasi:

1. identificazione di tutti i documenti da trasferire;
2. estrazione dei protocolli di tutti i documenti da inserire nell'ambiente di conservazione con i dati di classificazione relativi;
3. creazione di supporti, in base a regole dimensionali e/o temporali stabilite dal responsabile della conservazione sostitutiva in fase di configurazione, per ognuna delle tipologie suindicate;
4. creazione, per ogni supporto, di una lista riassuntiva degli stessi con l'indicazione per ogni documento dell'identificativo univoco del documento (hash).

Al termine del processo di creazione del supporto, il responsabile della conservazione completa il processo di archiviazione sostitutiva mediante l'apposizione della firma digitale e marcatura temporale sul file d'indice.
Ogni scheda documentale relativa a documenti sottoposti a conservazione digitale viene bloccata e resa immodificabile dal sistema, se non per le funzioni caratterizzanti il flusso di lavorazione, quali le annotazioni elettroniche, allegati non ufficiali, assegnazione, visibilità.

Per la gestione dei documenti trasferiti nell'archivio di conservazione, il sistema rende disponibili al conservatore le seguenti funzioni:

- ricerca dei documenti;
- ricerca sui supporti di documenti;
- estrazione di un supporto rimuovibile consultabile autonomamente;
- controllo di validità della marca temporale;
- aggiornamento della marca temporale.

Tipologia documentale	Protocollo in ingresso		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Protocollo	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Protocollo Ufficiale	

Tipologia documentale	Protocollo in uscita		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Protocollo	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Protocollo Ufficiale	

Tipologia documentale	Scheda Registrazioni		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Progressivo	Si	Si
	Archivio	Si	Si
	Data Registrazione	Si	Si
	Nome File	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Protocollo Ufficiale	

8.4.2. Registri di archivio

Oltre al registro di protocollo ufficiale e al registro giornaliero di protocollo, con le relative tipologie documentali, sono sottoposti a conservazione anche gli archivi relativi a registrazione particolare, ovvero i cd. registri di archivio, seguendo la medesima cadenza giornaliera.
L'obiettivo è di porre in conservazione le tipologie documenti a carattere ufficiale dell'Istituto, quali le Delibere, le Disposizione, gli Ordini di Servizio (OdS) e i Verbali.

Tra questi archivi sono considerati nel medesimo processo di conservazione anche le tipologie documentali incluse nei registri di Predisposizione e di Lavoro, con cadenza giornaliera – analoga al registro di protocollo – ma con un intervallo di conservazione ben più ampio (almeno a 120 giorni), in quanto sono considerati conservabili quei documenti che, pur nel loro stato di lavorazione e trattazione, ovvero in attesa di approvazione, rappresentano un ciclo di vita documentario concluso e da sottoporre a conservazione.

Le relative schede documentali sono contestualmente rese immodificabili, fatte salve le operazioni relative al flusso di lavorazione (annotazioni, assegnazioni, visibilità, etc.).

Tipologia documentale	Delibere Ufficiali		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Numero Delibera	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Delibere	

Tipologia documentale	Disposizioni Ufficiali		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Numero Disposizione	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Disposizioni	

Tipologia documentale	Verbali Ufficiali		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Numero Verbale	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	Verbali	

Tipologia documentale	OdS Ufficiali		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Numero OdS	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data protocollo	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	2 giorni	
	Registro	OdS	

Tipologie documentali	Comunicazioni in uscita; Comunicazioni interne; Delibere; Disposizioni; OdS; Verbali		
Metadati	**Nome attributo**	**Conservato**	**Visualizzati**
	Numero Documento	Si	Si
	Archivio	Si	Si
	Titolo	Si	Si
	Classe	Si	Si
	Data documento	Si	Si
	Oggetto	Si	Si
Proprietà	**Tipo Proprietà**	**Valore**	
	Massimario di scarto	*cfr. A1*	
	Durata conservazione (aa.)	*cfr. A1*	
	Intervallo conservazione (gg.)	120 giorni	
	Registro	Predisposizione	

8.5. Modalità di presa in carico di uno o più pacchetti di versamento

8.5.1. Accettazione (pacchetto di versamento)

Il servizio di *Accettazione* è configurato per accedere direttamente su DEMACO e preleva i documenti dei seguenti archivi:

- Registro Protocollo Ufficiale: le tipologie documentali protocollo in ingresso e protocollo in uscita;
- Registro Giornaliero di Protocollo: contenente i documenti della tipologia documentale "Scheda Registrazioni";
- Registri di Archivio, contenenti i documenti delle seguenti tipologie documentali: "Comunicazioni in uscita e interne" (del registro di predisposizione); "Delibere Ufficiali"

(del registro delibere); “Disposizioni Ufficiali” (del registro disposizioni), Verbali Ufficiali (del registro verbali), OdS Ufficiali (del registro Ods).

Le impostazioni delle modalità di esecuzione hanno orari predefiniti e sono eseguiti attraverso procedure automatiche.

Attraverso l’interfaccia web del sistema è possibile verificare l’elenco dei documenti con lo stato in accettazione (ovvero l’equivalente del rapporto di versamento) finalizzata alla successiva fase di conservazione.

8.5.2. Creazione (pacchetto di archiviazione)

Il servizio di creazione è specializzato secondo i seguenti modelli:

- Modello “Supporto documenti Protocollo in ingresso”;
- Modello “Supporto documenti Protocollo in uscita”;
- Modello “Supporto documenti Registro Giornaliero di protocollo”;
- Modello “Supporto documenti Registri di archivio”.
- Modello “Supporto documenti Registro di lavoro e Predisposizione”

Le caratteristiche principali dei modelli sopra elencati sono:

Modello “Supporto documenti Protocollo in ingresso”	
Nome supporto	*<nome tipologia documentale> - <progressivo univoco supporto>*
Tipologia documentale	Protocollo in ingresso
Modalità attivazione	Manuale e automatica
Verifica dei documenti	*Impronta* (non sarà verificata la validità della firma sui documenti, in quanto tale verifica è già eseguita da DEMACO).
Modello di materializzazione	Due copie di backup
Modello di certificazione supporto	Firma del responsabile e riferimento temporale
Numero massimo di documenti nel supporto	-
Dimensione massima del supporto (MB)	600 MB
Soglie: Numero	-
Soglie: Dimensione documenti	-
Soglie: tempo dall’ultimo supporto creato (gg.)	2 giorni
Soglie: tempo dal documento più prossimo alla scadenza	-

Modello “Supporto documenti Protocollo in uscita”	
Nome supporto	*<nome tipologia documentale> - <progressivo univoco supporto>*
Tipologia documentale	Protocollo in uscita
Modalità attivazione	Manuale e automatica
Verifica dei documenti	*Impronta* (non sarà verificata la validità della firma sui documenti, in quanto tale verifica è già eseguita da DEMACO).

Modello di materializzazione	Due copie di backup
Modello di certificazione supporto	Firma del responsabile e riferimento temporale
Numero massimo di documenti nel supporto	-
Dimensione massima del supporto (MB)	600 MB
Soglie: Numero	-
Soglie: Dimensione documenti	-
Soglie: tempo dall'ultimo supporto creato (gg.)	2 giorni
Soglie: tempo dal documento più prossimo alla scadenza	-

Modello "Supporto documenti Registro Giornaliero di protocollo"	
Nome supporto	*Documenti Registri Giornalieri di protocollo - <progressivo univoco supporto>*
Tipologia documentale	Registro Giornaliero di protocollo.
Modalità attivazione	Manuale e automatica
Verifica dei documenti	*Impronta* (non sarà verificata la validità della firma sui documenti, in quanto tale verifica è già eseguita da DEMACO).
Modello di materializzazione	Due copie di backup
Modello di certificazione supporto	Firma del responsabile e riferimento temporale
Numero massimo di documenti nel supporto	-
Dimensione massima del supporto (MB)	600 MB
Soglie: Numero	-
Soglie: Dimensione documenti	-
Soglie: tempo dall'ultimo supporto creato (gg.)	2 giorni
Soglie: tempo dal documento più prossimo alla scadenza	-

Modello "Supporto documenti Registri di archivio"	
Nome supporto	*Documenti Registri di archivio - <progressivo univoco supporto>*
Tipologia documentale	Delibere, Disposizioni, OdS, Verbali (Ufficiali)
Modalità attivazione	Manuale e automatica
Verifica dei documenti	*Impronta* (non sarà verificata la validità della firma sui documenti, in quanto tale verifica è già eseguita da DEMACO).
Modello di materializzazione	Due copie di backup
Modello di certificazione supporto	Firma del responsabile e riferimento temporale

Numero massimo di documenti nel supporto	-
Dimensione massima del supporto (MB)	600 MB
Soglie: Numero	-
Soglie: Dimensione documenti	-
Soglie: tempo dall'ultimo supporto creato (gg.)	2 giorni
Soglie: tempo dal documento più prossimo alla scadenza	-

Modello "Supporto documenti Registro di lavoro e Predisposizione"	
Nome supporto	*Documenti in Predisposizione e Registro di lavoro - <progressivo univoco supporto>*
Tipologia documentale	Documenti di lavoro; Comunicazioni in uscita e interne, Delibere, Disposizioni, OdS, Verbali (in Predisposizione)
Modalità attivazione	Manuale e automatica
Verifica dei documenti	*Impronta* (non sarà verificata la validità della firma sui documenti, in quanto tale verifica è già eseguita da DEMACO).
Modello di materializzazione	Due copie di backup
Modello di certificazione supporto	Firma del responsabile e riferimento temporale
Numero massimo di documenti nel supporto	-
Dimensione massima del supporto (MB)	600 MB
Soglie: Numero	-
Soglie: Dimensione documenti	-
Soglie: tempo dall'ultimo supporto creato (gg.)	120 giorni
Soglie: tempo dal documento più prossimo alla scadenza	-

8.6. Modello di conservazione e del trattamento dei pacchetti di archiviazione

Il modello definito per la certificazione valido per le tipologie sopra elencate è impostato come segue:

Modello "certificazione con Firma e Rif. Temporale"	
Modalità attivazione	Manuale
	Automatica
Operazioni abilitate	Firma (manuale)
	Riferimento temporale (automatica)
Modalità di esecuzione	Intervalli regolari

Per utilizzare la lista delle *Certification Authority*, disponibile sul sito dell'Agenzia per l'Italia Digitale, è controllata per ogni verifica la lista dei certificatori attivi; l'attività comporta una connessione da parte dell'*application server* verso l'esterno.

La firma può essere verificata nelle fasi di: accettazione, creazione supporti (pacchetto di versamento); certificazione e materializzazione (pacchetto di archiviazione).
Il controllo della validità della firma in fase di accettazione verifica la validità del certificato (scaduto, revocato); in caso di individuazione di un'anomalia viene notificato il problema nel report generato dalla fase, per le valutazione da parte del RSP, o suoi delegati.

8.7. Modello di monitoraggio del sistema e degli archivi

Il modello definito per il monitoraggio dei supporti e dei documenti per le tipologie sopra elencate è impostato come segue:

Modello "monitoraggio completo"	
Modalità di esecuzione	ad orari predefiniti
Intervallo scadenza (gg.)	1 giorno
Intervallo segnalazione (ore)	1 ora
Intervallo cancellazione segnalazioni (gg.)	10 giorni

Tipo monitoraggio	**Abilitato**
Monitoraggio che controlla presenza di documenti in scadenza	Si
Monitoraggio che controlla presenza di supporti in scadenza o da ricertificare	Si
Monitoraggio generico su documenti e supporti: controlla impronta del documento/supporto originale	Si
Monitoraggio generico su documenti e supporti: controlla impronta del documento/supporto materializzato	Si

Riferimento temporale: InfoCert.
Controllo firma: accesso all'esterno (HTTP).

Il responsabile della conservazione, o suoi delegati, verifica la corretta funzionalità del sistema e dei programmi di gestione per il sistema di conservazione; la funzione di controllo si svolge mediante gestione delle eccezioni.

Per ogni supporto di conservazione è effettuato annualmente un controllo sullo stato di conservazione. Tale processo prevede una verifica preliminare della effettiva leggibilità del supporto virtuale sul quale è memorizzato l'archivio, seguita dalla visualizzazione, a campione, dei documenti in esso contenuti.

Non oltre cinque anni a decorrere dalla data di messa in conservazione, l'integrità di tutti i supporti e la fruibilità di tutti i documenti conservati devono essere controllati, procedendo ove necessario a riversamento diretto o sostitutivo.

8.8. Modello di esportazione di duplicati o copie (pacchetto di distribuzione)

Il modello definito per la materializzazione dei supporti per le tipologie sopra elencate è impostato come segue:

Modello "materializzazione"			
Modalità di esecuzione	Intervalli regolari		
Tipo supporto	File system		
Periferiche	**Nome logico**	**Visualizza con CD viewer**	**Crea Iso**
	Copia 1	Si	No
	Copia 2	Si	No
	Repository distribuzione	Si	Si

8.9. La sicurezza nella conservazione dei documenti informatici

8.9.1. Le misure previste

Al fine di garantire la sicurezza e la continuità dei servizi, l'attenzione è rivolta principalmente ai seguenti profili:

- controllo e mantenimento delle strutture hardware e software necessarie per lo svolgimento dell'attività relativa alla conservazione sostitutiva;
- fornitura di un servizio di gestione degli spazi su disco di rete per gli archivi dati e organizzazione dei salvataggi periodici dei dati con archiviazione in luogo sicuro delle copie effettuate;
- continuità di erogazione del servizio di utilizzo dei server, in base ai tempi ed alle modalità concordate e compatibilmente con le attività di manutenzione tecnica dei sistemi;
- salvaguardia della riservatezza dell'informazione elettronica, riducendo a livelli accettabili il rischio che un'entità non autorizzata possa accidentalmente o deliberatamente accedere all'informazione stessa;
- integrità della documentazione archiviata in modo elettronico, riducendo a livelli accettabili il rischio di alterazioni o cancellazioni di informazioni da parte di soggetti non autorizzati o fenomeni non controllabili (deterioramento dei supporti magnetici o ottici, malfunzionamenti delle unità di memorizzazione, etc.);
- disponibilità dell'informazione archiviata in modo elettronico.

Per il requisito di "accesso e consultazione", il conservatore garantisce la leggibilità nel tempo di tutti i documenti sulla base dei formati previsti dalle regole tecniche vigenti.

Per ogni aspetto della sicurezza non incluso in questa sezione si rimanda al capitolo 9.

8.9.2. Tracciamento degli accessi

Le operazioni previste dai flussi documentali descritti nel presente documento sono tracciate in

appositi log, consultabili attraverso una consolle di gestione. I dati di ogni supporto virtuale prodotto sono memorizzati sul sistema e sono memorizzati nel supporto stesso ed archiviato insieme al file di versamento, firmato e marcato, contenente le impronte dei documenti conservati.

L'accesso al sistema di archiviazione e conservazione sostitutiva dalle postazioni di lavoro segue la politica di sicurezza adottata dall'Istituto; è regolato da una procedura di autenticazione che permette di verificare l'identità della persona e, quindi, di accertare che essa sia in possesso delle credenziali di autenticazione per l'accesso.

8.9.3. Conservazione dei documenti riservati

Nel sistema di conservazione i documenti sono conservati in forma cifrata. Il sistema ha la chiave di cifratura per la gestione e il controllo del processo di conservazione, a cui può accedere il RSP, o suoi delegati. Il sistema di gestione documentale e quello di conservazione fanno riferimento a un duplicato del medesimo documento.

8.9.4. Accesso al sistema di conservazione

Il sistema di conservazione è accessibile in modalità fisica e logica esclusivamente al responsabile della conservazione e al responsabile della gestione documentale, e relativi delegati, d'intesa con il responsabile della sicurezza.

In caso di accesso per esigenze di manutenzione, il responsabile della conservazione o il responsabile della gestione documentale, o suoi delegati, d'intesa con il responsabile della sicurezza, autorizza l'attività e ne traccia l'intervento, a garanzia dell'integrità e della riservatezza dei documenti e dei dati posti in conservazione.

9. Gestione in sicurezza dei documenti informatici

9.1. Principi generali

Il presente capitolo riporta le misure di sicurezza adottate nel sistema DEMACO per la formazione, 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.

Con riferimento alle norme riportate nel documento "Sicurezza delle dotazioni informatiche – norme per gli utenti" (disponibile nella intranet dell'Istituto), le credenziali di accesso al sistema (utente e password) rappresentano il riconoscimento univoco del dipendente, in base ai requisiti di sicurezza.

9.2. Misure generali di sicurezza per la gestione documentale

Le misure generali tecniche e organizzative inerenti alla gestione documentale, in accordo allo standard ISO/IEC 27001 e con riferimento al documento "Politica di sicurezza della rete. Criteri minimi di sicurezza della infrastruttura telematica CONSOB" (cfr. A2 – Normativa di riferimento e bibliografia), sono le seguenti:

- protezione periferica della Intranet della CONSOB;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di dematerializzazione DEMACO, 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;
- gestione delle situazioni di emergenza da parte di un gruppo di risorse interne qualificate (*task force*);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura degli oggetti documentali (documenti, allegati, etc.) del sistema archiviati nell'infrastruttura informatica, allo scopo di renderli inintelligibili anche a chi è autorizzato ad accedervi per le attività di manutenzione;

- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

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 dematerializzazione DEMACO sono consultabili in caso di necessità dal RSP, o suoi delegati, ed è sottoposto a tracciamento.

9.3. Formazione dei documenti – Aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici gestiscono:

- l'identificabilità della CONSOB e del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi della normativa vigente;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della CONSOB, con altre AOO e con soggetti esterni.

I documenti CONSOB 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'Istituto 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.

9.4. Gestione dei documenti informatici – Aspetti di sicurezza

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

- l'accesso esclusivo al server del sistema di dematerializzazione DEMACO 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 DEMACO:

- 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 dalla CONSOB 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.

9.4.1. Componente organizzativa della sicurezza

Questa sezione si riferisce alle attività svolte nell'ambito del sistema DEMACO.

In particolare, la definizione delle misure di sicurezza nell'ambito del sistema è proposta dalle strutture di sicurezza informatica, d'intesa con il RSP o suoi delegati.

9.4.2. Componente fisica

Il controllo degli accessi ai luoghi fisici in cui sono custodite le risorse infrastrutturali di DEMACO e le relative misura di sicurezza sono regolati secondo i seguenti criteri basati su due livelli:

- l'accesso alla sede CONSOB avviene tramite badge dell'Istituto, rilasciato per i dipendenti e per gli ospiti previa identificazione;
- l'accesso alla sala server può avvenire esclusivamente con badge dell'Istituto appositamente abilitato.

9.4.3. Componente logica e infrastrutturale

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

Tali componenti sono rappresentate attraverso apposite procedure interne finalizzate alle "politiche di sicurezza della rete" e alla "sicurezza delle dotazioni informatiche" (cfr. A2 – Normativa di riferimento e bibliografia).

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:

- *Advanced Document Protection* che, tramite *file system encryption*, garantisce che i documenti archiviati nel sistema non possano essere consultati in modo non controllato mediante l'accesso diretto allo *storage* fisico che li contiene; viene eseguita la cifratura dei dati e dei documenti sia durante la comunicazione con i *client* che in fase di memorizzazione dei documenti stessi;
- *Document Digest Protection* che, tramite "impronta" (*hash*) dei *file*s, garantisce che un documento archiviato non possa essere sostituito o modificato in modo non controllato mediante l'accesso diretto allo *storage* fisico che lo contiene;

- 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 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).

9.4.4. Gestione della riservatezza

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

Sono previsti cinque livelli di riservatezza così definiti:
- livello 0: pubblico (ad es. esportabile su internet);
- livello 1: a diffusione interna (ad es. esportabile solo su intranet CONSOB);
- livello 2: non riservato;
- livello 3: riservato;
- livello 4: segreto (visibile agli utenti appartenenti ad un gruppo specifico).

Un documento di un certo livello è consultabile da tutti gli utenti aventi diritto di visibilità per quel livello o superiore 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.
I documenti, indipendentemente dal livello di riservatezza, sono comunque cifrati e sono visibili solo agli utenti assegnatari del documento stesso.

L'impostazione del livello di riservatezza è obbligatorio e si basa sulle seguenti regole:
- il livello zero relativo ai documenti a pubblica diffusione è impostato di default;
- qualsiasi utente può cambiare il livello di riservatezza di un documento di livello zero;
- solo gli aventi diritto sul livello impostato, o superiore, possono diminuire o aumentare il livello di riservatezza del documento.

L'impostazione del livello di riservatezza ha una sua data di scadenza (predefinita dal sistema) che è configurabile dall'utente, ad eccezione dei primi due livelli che non prevedono tale data. Allo scadere di tale tempo il documento è automaticamente portato al livello immediatamente inferiore di riservatezza: questo *downgrade* automatico della riservatezza è applicato a tutti i documenti di livello superiore al primo; pertanto un documento al primo livello di riservatezza non può passare automaticamente a livello pubblico.
Il sistema traccia la storia della variazione dei cambiamenti relativi alla riservatezza del documento, memorizzando sia le informazioni sull'impostazione che la modifica del livello di riservatezza, ivi incluso il downgrade automatico per raggiunta scadenza della riservatezza.

9.4.5. Gestione dei tracciamenti

I tracciamenti di sicurezza sono costituiti da informazioni relative, ad es. ai dati o alle transazioni -presenti o transitate su DEMACO - 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 DEMACO;
- 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 DEMACO.

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

- i log di sistema sono tracciati nella storia delle schede documentali e archiviati a cadenza periodica, fino al passaggio del documento e della scheda al sistema di conservazione;
- un estratto delle informazioni di tracciamento, di cui al punto precedente, sono trasmessi in apposito sistema di sicurezza e conservati in storage dedicato con una finestra temporale di *retention* non inferiore a 6 mesi;
- 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.

9.5. 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 CONSOB, 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 della CONSOB mediante posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nelle procedure interne di sicurezza (cfr. A2 – Normativa di riferimento e bibliografia)

9.6. 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 di dematerializzazione DEMACO.

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

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

- 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.

9.6.1. 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.
- *Service desk*, che ha la visibilità dei metadati relativi a tutte le schede documentali.
- *Utente generico*, che ha la visibilità per competenza o per conoscenza delle schede documentali secondo i profili di assegnazione.

9.6.2. 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 che per la disattivazione delle utenze con profilo di accesso *Utente generico*.

La creazione di nuove utenze di *Amministratore* e/o di *Service desk* 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.

9.6.3. Utenti interni

Ciascun utente interno di DEMACO 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 da CONSOB. 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 RSP di CONSOB, o da suoi delegati.

Ulteriori elementi di abilitazione al sistema sono descritti nell'ambito della procedura interna relativa alla riservatezza (cfr. A2 – Normativa di riferimento e bibliografia).

9.6.4. Utenti esterni

L'accesso al sistema di dematerializzazione 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 dalla CONSOB (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 sono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

L'eventuale accesso a DEMACO 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'Istituto sono fornite le informazioni necessarie per accedere a detti documenti amministrativi.

9.7. Politiche di sicurezza adottate dalla CONSOB

Le politiche di sicurezza, come da procedure interne riportate in A2 – 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 di dematerializzazione DEMACO.

Il RSP, 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.

9.8. Manutenzione ordinaria ed aggiornamenti

Allo scopo di garantire la continuità del servizio, si prevede un piano di manutenzione programmata del sistema utilizzato, che ne riduce al minimo le alterazioni e ne preserva la funzionalità.
In assenza di specifiche inefficienze, l'aggiornamento del software è rilasciato per rispondere ad esigenze frutto di modifiche o novità in ambito normativo. Il responsabile del sistema ha cura di far mantenere un archivio delle diverse versioni del software e dei relativi programmi necessari alla fruizione dei documenti.
Per quanto riguarda i dispositivi di firma digitale utilizzate, è tenuta traccia della relativa scadenza associata a ciascuno di essi.

9.9. Gestione di eventi eccezionali

Sono di seguito descritte le linee generali delle modalità adottate per fronteggiare eventi eccezionali nell'ambito del processo di gestione dei sistemi.

L'elemento essenziale posto alla base delle politiche di gestione, in tale contesto, è il principio di alta affidabilità, applicata a tutte le strutture di carattere tecnologico.

1. *Guasti dei server*
   In generale, l'ambiente operativo è strutturato in modo tale da garantire la sicurezza della integrità e della reperibilità dei dati anche a fronte di malfunzionamenti improvvisi delle apparecchiature utilizzate. Di norma, sono attive almeno due macchine virtuali e due macchine fisiche diverse: in questo modo è sempre garantita la possibilità, per documenti ed operazioni, di migrare da una struttura difettosa ad una correttamente funzionante. Il ripristino in caso di guasto viene governato da piani previsti dalle politiche di gestione in essere, tramite il recupero dei dati da backup aziendali pianificati: esso avviene tramite l'ultima copia del backup completo e tutte le copie dei backup incrementali fino al momento dell'interruzione.

2. *Compromissione del software*
   La funzionalità del sistema è gestita e supervisionata dal RSP e dai suoi delegati. In caso di guasto, la versione in uso del software può essere ripristinata tramite i backup aziendali o, qualora ciò non fosse possibile, tramite nuova installazione sulla macchina.

3. ***Inaccessibilità al sito della Certification Authority***
   La Certification Authority designata per fornire i propri servizi implementa politiche di continuità di erogazione previste dalla normativa vigente. Nel caso di compromissione del sito dell'ente certificatore, il servizio per questa fase può subire temporanee interruzioni.

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

10. Approvazione e aggiornamento del Manuale di gestione

10.1. Modalità di approvazione e aggiornamento

Il Manuale, in sede di prima adozione, è approvato dalla Commissione su proposta del RSP.

Il presente Manuale sarà aggiornato direttamente dal RSP 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 RSP si avvale dei propri delegati, ovvero dei funzionari idonei per competenze ed esperienze.

Ogni altra modifica sarà sottoposta ad approvazione da parte della Commissione.

10.2. 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'Istituto mediante la rete intranet;
- inviata, per conoscenza, all'AgID, Agenzia per l'Italia Digitale.

10.3. Entrata in vigore del presente Manuale

Le prescrizioni del presenta Manuale trovano applicazione dal 1° luglio 2014.

ADDENDA

A1 – Linee guida per gli archivi di deposito e storico

In questa sezione sono enunciati i principi e descritte le procedure relative alla formazione e gestione degli archivi di deposito e storico e alla consultazione delle serie, dei fascicoli e dei documenti conservati.
Si fa qui particolare riferimento alla documentazione analogica e si rinvia al capitolo 8 per l'illustrazione dei principi e delle procedure inerenti al sistema di conservazione digitale.
Tuttavia, nella comprensione del concetto unitario di archivio centrale di CONSOB, sono qui enunciati principi che governano la gestione della documentazione a prescindere dal supporto sul quale è registrata e trasmessa l'informazione.

1. Archiviazione della documentazione

Con l'avvio del processo di dematerializzazione, il RSP, o suoi delegati, ha individuato in appositi locali delle sedi di Roma e Milano il luogo di conservazione dell'archivio corrente e di deposito. La scelta è stata effettuata a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza).

Gli addetti al Protocollo gestiscono l'archiviazione della documentazione analogica corrente ricevuta dall'Istituto. L'archiviazione avviene attraverso l'ordinata raccolta per numero di protocollo di documenti e supporti magneto-ottici in faldoni. Ogni faldone riporta, sul dorso, oltre al numero identificativo, il primo e l'ultimo numero di protocollo della documentazione contenuta.

Qualora i documenti protocollati non scansionabili siano stati inviati in originale al destinatario, è lasciato disponibile un adeguato spazio nel faldone per la sua archiviazione, che avverrà nel momento in cui il documento non sarà più necessario per la conduzione del procedimento o dell'attività. È cura del RdP far trasmettere il documento analogico al Protocollo per la sua archiviazione non appena esaurita la sua utilità ai fini del procedimento o dell'attività svolti.

2. Formazione e gestione dell'archivio di deposito

L'archivio di deposito è dislocato nelle sedi dell'Istituto di Roma e Milano, nonché presso i locali messi a disposizione di due società specializzate in *outsourcing*.

L'archiviazione a deposito dei fascicoli cartacei chiusi, che hanno avuto avvio in data antecedente al 1° luglio 2013, devono essere trasferiti nell'archivio di deposito entro 18 mesi dalla data di chiusura del fascicolo stesso, ovvero entro 18 mesi dall'entrata in vigore del Manuale. Per quanto concerne i fascicoli "ibridi" si rimanda a quanto precedentemente disposto (cfr. paragrafo 7.13).

L'archivio corrente della documentazione cartacea presso il Protocollo trattata dal 1° luglio 2013, con l'avvio del sistema DEMACO, viene trasferito all'archivio di deposito contestualmente alla digitalizzazione dei documenti.

I fascicoli che riguardano il personale devono essere trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio del dipendente cui si riferiscono.

Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Prima di effettuare il trasferimento, la UO e/o il RdP oppure, successivamente, il RSP, o suoi delegati, procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- della corretta indicazione della data di chiusura sulla copertina del fascicolo. Nel caso di fascicolo ibrido, sulla copertina si indica anche il rifermento al fascicolo digitale DEMACO.

Il RSP, o suoi delegati, provvede inoltre:

- all'eventuale scarto di copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza dei documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli, il RSP, o suoi delegati, predispone o fa predisporre l'elenco di versamento (ovvero l'elenco dei protocolli presenti nei fascicoli, elenco dei fascicoli archiviati e la relativa consistenza e movimentazione) da inviare all'archivio di deposito e copia di detto elenco viene conservata dal responsabile. Il RSP, o suoi delegati, è a conoscenza della collocazione del materiale archivistico, degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e dei movimenti delle singole unità archivistiche.

Nel caso di fascicolo "ibrido", l'utente si limiterà a chiudere il fascicolo in DEMACO e il correlativo cartaceo e a trasmettere quest'ultimo secondo quanto disposto nel presente paragrafo e nel paragrafo 07.13.

Le copie a stampa della documentazione digitale prodotta in DEMACO non hanno valenza a carattere amministrativo per le finalità di archiviazione cartacea.

3. Scarto, selezione e riordino dei documenti

3.1. Operazioni di selezione

Nell'ambito dell'archivio di deposito viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che CONSOB non ritiene più opportuno conservare ulteriormente, allo scopo di garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità organizzativa e pratica di conservare indiscriminatamente ogni documento.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica, culturale e scientifica.

A seguito dell'avvio del processo di dematerializzazione DEMACO, CONSOB sulla base della pianificazione pluriennale predispone il "massimario di selezione". Il massimario viene proposto

dal RSP alla Soprintendenza archivistica di competenza e viene approvato con atto formale dalla Commissione.

3.2. Procedura per lo scarto legale dei documenti

Anche in presenza di un massimario, risulta indispensabile seguire l'iter previsto dalla normativa sullo scarto come procedimento amministrativo.

L'iter procedimentale da seguire è il seguente:

1. Decisione (periodica) di procedere alle operazioni di selezione;
2. Istruzione del procedimento e redazione dell'elenco;
3. Provvedimento che approva la proposta di scarto da trasmettere alla Soprintendenza archivistica;
4. Autorizzazione delle Soprintendenza archivistica;
5. Consegna della documentazione alla Croce Rossa Italiana / Termodistruzione e verbale di avvenuta distruzione.

In sostanza, serve una decisione periodica e programmatica da parte di CONSOB di effettuare lo scarto di documenti, di fascicoli e di serie ritenuti non più occorrenti alle esigenze amministrative e storiche.

La proposta deve contenere le indicazioni relative alla tipologia di scarto, quali: totale; per sfoltimento; per campionatura, etc.

Deve quindi essere redatta la proposta di scarto (elenco di selezione), nella quale sono indicati:

- la quantità del materiale (buste, registri, pacchi, scatoloni, …) espresso in metri lineari e il relativo peso, ovvero nel caso di scarto di documenti digitali il valore in gigabyte o terabyte;
- la classificazione;
- la descrizione del materiale;
- gli estremi cronologici;
- la motivazione.

L'elenco dei documenti che si propongono per lo scarto è parte integrante del provvedimento, da trasmettere alla Soprintendenza archivistica, che formulerà eventuali osservazioni e rilascerà l'autorizzazione allo scarto. Ottenuta l'autorizzazione, si potrà procedere alla materiale e irreversibile distruzione degli atti. Il procedimento si conclude con la trasmissione alla Soprintendenza archivistica del verbale di avvenuto scarto.
Le operazioni di selezione e scarto sono effettuate, sotto la vigilanza del RSP, o suoi delegati (ovvero da persona incaricata), a cura degli addetti preposti.

Le procedure sopra descritte possono essere applicate anche per la selezione e lo scarto della documentazione digitale.

3.3. Riordino e conservazione della documentazione

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita da CONSOB e consiste nella schedatura dei materiali e nell'organizzazione delle schede.

L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (scatole, pallets, etc.) che riportano all'esterno l'indicazione del contenuto, la

classificazione e i tempi di conservazione dei documenti.

Le operazioni di riordino sono applicate anche alla documentazione digitale.

4. Versamento dei documenti nell'archivio storico

CONSOB, sulla base delle normative in vigore e del piano pluriennale in corso di definizione, trasferisce all'archivio storico i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.

I trasferimenti vengono effettuati dopo il completamento delle operazioni di selezione e scarto.

5. Consultazione da parte di utenti esterni

5.1. Consultazione per finalità giuridico-amministrative

Il diritto di accesso ai documenti conservati nell'archivio di deposito di CONSOB è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 e successive modifiche.

5.2. Consultazione per finalità culturali, storiche e scientifiche

La richiesta di consultazione di documenti dell'archivio storico per finalità culturali, storiche e scientifiche sarà disciplinata da CONSOB, anche sulla base della pianificazione pluriennale del processo di dematerializzazione DEMACO.
La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, sulla base della regolamentazione interna in materia di riservatezza. È possibile l'ammissione alla consultazione dei documenti riservati, secondo le vigenti disposizioni in materia di diritto di accesso;
- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

La domanda di accesso ai documenti viene presentata a CONSOB, che provvede a smistarla al servizio competente. Le procedure per la consultazioni saranno oggetto di successiva regolamentazione interna.

6. Consultazione da parte di personale interno a CONSOB

Le UO, per motivi di consultazione, possono richiedere in ogni momento al servizio competente i fascicoli conservati nella sezione archivistica di deposito o storica.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio della medesima UO od altra UO avviene solamente per il tempo necessario all'esaurimento di un'attività o di un procedimento amministrativo. Nel caso di accesso ad archivi cartacei, l'affidamento temporaneo avviene mediante richiesta scritta, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, la sua UO e la sua firma.
Una copia o duplicato della richiesta di consultazione è conservata all'interno del fascicolo, l'altra nella posizione fisica occupata dal fascicolo cartaceo in archivio.

Tale movimentazione viene registrata in un apposito registro di carico e scarico dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata. Il RSP, o suoi delegati, verifica che la restituzione dei fascicoli affidati avvenga alla scadenza prevista.
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo originario.

Nel caso di accesso ad archivi informatici, sulla base delle attività di pianificazione in corso di definizione, le richieste potranno avvenire per via telematica: saranno stabilite da CONSOB le politiche e le procedure di accesso alle informazioni.

In ogni caso sarà garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione/cancellazione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

A2 – 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

CNIPA Deliberazione del 19 febbraio 2004, n. 11
Regole tecniche per la riproduzione e conservazione di documenti su supporto idoneo a garantire la conformità dei documenti agli originali

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

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

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

2. Letteratura grigia

Circolare della Presidenza del Consiglio dei Ministri del 20 aprile 2001, n. 1.1.26/10888/9.92
Regole e raccomandazioni per la formulazione tecnica dei testi legislativi

Circolare della Presidenza del Consiglio Dei Ministri del 2 maggio 2001, n. 1/1.1.26/10888/9.92
Guida alla redazione dei testi normativi

CNIPA Quaderno n. 21 del febbraio 2006
Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle pubbliche amministrazioni. Modello di riferimento

CNIPA (a cura di), *La dematerializzazione della documentazione amministrativa. Libro Bianco del Gruppo di Lavoro interministeriale per la dematerializzazione della documentazione tramite supporto digitale*, marzo 2006

CNIPA Quaderno n. 25 dell'aprile 2006
La dematerializzazione della documentazione amministrativa

Scuola Superiore della Pubblica Amministrazione, a cura di E. Aga Rossi, M. Guercio, *La metodologia per la definizione dei piani di classificazione in ambiente digitale*, Roma, 2005.

Commissione Europea - Ufficio delle Pubblicazioni
Manuale interistituzionale di convenzioni redazionali, http://publications.europa.eu/code/it/it-000100.htm

3. Regolamentazione interna

Delibera n. 9642 del 13 dicembre 1995
Disposizioni concernenti misure organizzative per l'esercizio del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 22, comma 3, della legge 7agosto 1990, n. 241 e del DPR 27 giugno 1992, n. 352

Regolamento del personale CONSOB (adottato dalla Commissione con deliberazione n. 13859 del 4 dicembre 2002, resa esecutiva con d.p.c.m. del 30 dicembre 2002 e successivamente modificato con delibere n. 14604 del 16 giugno 2004, resa esecutiva con d.pc.m. del 15 luglio 2004; n. 15091 del 22 giugno 2005, resa esecutiva con d.p.c.m. del 14 luglio 2005; n. 15252 del 14 dicembre 2005, resa esecutiva con DPCM del 28 dicembre 2005; n. 15548 del 7 settembre 2006, resa esecutiva con DPCM del 22 settembre 2006; n. 16782 del 2 febbraio 2009, resa esecutiva con DPCM del 23 febbraio 2009 e n. 17832 e n. 17833 del 22 giugno 2011, rese esecutive con DPCM del 15 luglio 2011.)

Delibera n. 18388 del 28 novembre 2012 e successivamente modificata con Delibera n. 18628 del 31 luglio 2013
Regolamento generale sui procedimenti amministrativi della Consob ai sensi dell'articolo 24 della legge 28 dicembre 2005, n. 262, e dell'articolo 2, comma 5, della legge 7 agosto 1990, n. 241 e successive modificazioni

Delibera n. 18554 del 29 maggio 2013
Approvazione del Titolario di classificazione

Disposizione del Direttore Generale n. 10 del 11 giugno 2013
Nomina del Responsabile per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi e del Responsabile della conservazione

Ordine di servizio n. 20 del 2013 del 25 giugno 2013
Avvio dell'operatività del sistema di dematerializzazione e gestione documentale DEMACO

Comunicazione al personale del 27 giugno 2013
Demaco - Dematerializzazione dei flussi documentali d'Istituto: delega di funzioni per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi nonché per la conservazione documentale

Documentazione organizzativa
Manuale della struttura, ver. del 5 ottobre 2012
Procedura di tutela delle informazioni Livello 4, ver. 2 del 31 ottobre 2013
Disposizione interna protocollo n. 12031699 del 20 aprile 2012 ad oggetto "Servizio corriere Roma-Milano: disposizioni interne per gli addetti al Settore Protocollo"

Documentazione di sicurezza
Politica di sicurezza della rete. Criteri minimi di sicurezza della infrastruttura telematica Consob, marzo 2012, ver. 1.0.
Sicurezza delle dotazioni informatiche. Norme per gli utenti, maggio 2012, ver. 1.4.

Ordine di servizio n. 10 del 15 marzo 2013
Modelli documentali standard con intestazione

Ordine di servizio n. 8 del 7 marzo 2014
Gestione dematerializzata dei flussi documentali d'Istituto (DEMACO): rilascio di versione aggiornata della relativa procedura

4. Bibliografia essenziale

Carucci Paola, *Il documento contemporaneo. Diplomatica e criteri di edizione*, Nuova Italia Scientifica, Roma, 1987

Carucci Paola, *Le fonti archivistiche. Ordinamento e conservazione*, La Nuova Italia Scientifica, Roma, 1983

Consiglio Internazionale Degli Archivi, *ISAD (G) - General International Standard Archival Description*, seconda edizione, 2000.

Consiglio Internazionale Degli Archivi, *ISAAR (CPF) – International Standard Archival Authority Record for Corporate Bodies, Persons and Families*, seconda edizione, 2004

Guercio Maria, *Archivistica informatica. I documenti in ambiente digitale*, Carocci, Roma, 2002

Gruppo di lavoro interistituzionale Aurora, *Le raccomandazioni di Aurora*, CLEUP, Padova, 2009

Gruppo di lavoro nazionale sui titolari delle università, I calzini del principe Carlo. Titulus 97 – I Titolari per gli archivi delle università italiane in vigore dal 1° gennaio 2007, CLEUP, Padova, 2007

ISO 8601, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 15489, *Information and documentation – Records management* (1. *General* e 2. *Guidelines*)

ISO 23081 - *Metadata for Records* (Part 1: Principles, Part 2: *Conceptual and implementation issues*, Part 3: *Self assessment method*)

DoD 5015.2-STD US Department of Defense: *Design Criteria Standard for Electronic Records Management Applications*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

Lodolini Elio, *Archivistica. Principi e problemi*, 9ª ed., Franco Angeli, Milano, 2000

Moreq. Requisiti modello per la gestione di record elettronici. Specifiche Moreq, trad. it., Bruxelles – Lussemburgo, 2001

The National Archives, *Managing electronic records without an Electronic Record Management System*, 2012

Penzo Doria Gianni, *Il fascicolo archivistico: le cinque tipologie e i modelli organizzativi*, in "Archivi & Computer", Fasc. 2-3, 2007, pp. 22-49

Penzo Doria Gianni, *Procedura, processo e procedimento: definizioni per la tabella dei procedimenti amministrativi ex l. 241/1990*, "Filo Diritto", 18 giugno 2013, www.filodiritto.com

5. Sitografia essenziale

Agenzia Digitale per l'Italia - http://www.agid.gov.it/

Associazione Nazionale Archivistica Italiana – ANAI – http://www.anai.org/anai-cms/

Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale – ANORC – http://www.anorc.it/index.php

Conseil International des Archives – ICA - http://www.ica.org/

DigitPA – Archivio - http://archivio.digitpa.gov.it/

Direzione Generale degli Archivi – DGA - http://www.archivi.beniculturali.it/

Dublin Core Metadata Initiative – http://dublincore.org/

Garante per la protezione dei dati personali – http://www.garanteprivacy.it/

Indice delle Pubbliche Amministrazioni – http://www.indicepa.gov.it/

Indice nazionale degli indirizzi PEC di professionisti e imprese – http://www.inipec.gov.it/

InterPARES Project – http://www.interpares.org

Posta Certificate@ del cittadino – http://www.postacertificata.gov.it/

The Library of Congress – Digital Preservertion – http://blogs.loc.gov/digitalpreservation/

A3 – Glossario

Archiviazione elettronica: processo di memorizzazione, su un idoneo supporto, di documenti informatici univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.
Conservazione dei documenti informatici: processo di conservazione dei documenti informatici mediante la loro memorizzazione su idonei supporti che garantiscano l'immodificabilità dei dati e termini con l'apposizione, sull'insieme dei documenti o su un'evidenza informatica (file XML di versamento) contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione, o suoi delegati, che attesta il corretto svolgimento del processo.
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.
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.
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.
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.
Registrazione di protocollo: memorizzazione, per ogni documento ricevuto o spedito, delle informazioni riguardanti il documento stesso.
Responsabile della conservazione sostitutiva: responsabile del corretto svolgimento del processo di conservazione dei documenti digitali (sia quelli formati direttamente in elettronico, sia le copie su supporto informatico dei documenti formati in origine su altro tipo di supporto ex art. 22 del CAD), nonché delle altre incombenze attribuitegli dalle leggi in materia.
Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: dirigente/funzionario a ciò preposto (v.).
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 protocollo informatico: insieme di programmi elaborativi e di archivi di dati che, insieme, costituiscono l'applicazione attraverso la quale l'Istituto assicura la gestione informatica della generalità dei propri documenti ex art. 52 del D.P.R. n. 445/2000.
Tab: indica una delle sezioni informative della scheda documentale del sistema DEMACO in cui sono riportati i metadati e le informazioni relative ai documenti informatici.

A4 – 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
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
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 – Codice dell'Istituto digitale
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)

Regolamento Camera di conciliazione e arbitrato - Delibera n. 18275 del 18 luglio 2012 e successive modificazioni

Regolamento Consulenti finanziari - Delibera n.17130 del 12 gennaio 2010 e successive modificazioni

Regolamento emittenti	Regolamento Consob n. 11971 di attuazione del decreto legislativo 24 febbraio 1998, n. 58 concernente la disciplina degli emittenti e successivi aggiornamenti.
Regolamento intermediari	Regolamento Consob n. 16190 recante norme di attuazione del decreto legislativo 24 febbraio 1998, n. 58 in materia di intermediari e successivi aggiornamenti.
Regolamento mercati	Regolamento Consob n. 16191 recante norme di attuazione del decreto legislativo 24 febbraio 1998, n. 58 in materia di mercati e successivi aggiornamenti.

Regolamento personale Consob - Delibera n. 13859 del 4 dicembre 2002 e successive modificazioni

Regolamento Amministrazione e contabilità - Delibera n. 10359 dell'11 dicembre 1996 e successive modificazioni

Provvedimenti interni

DEL	Delibera di Commissione
PRE	Atto a firma del Presidente
DG	Atto a firma del Direttore Generale
OdG	Ordine del Giorno
OdS	Ordini di Servizio
CaP	Comunicazioni al Personale
DIS	Disposizioni

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
TARSU	tassa per lo smaltimento dei rifiuti solidi urbani
TIA	tariffa di igiene ambientale
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
CoA	certificate of Approval
CONSOB	Commissione Nazionale per le Società e la Borsa
cs	carta dei servizi
DVD	digital versatile disc
EIP	ente di interesse pubblico
EMIR	European Market Infrastructure Regulation
ESMA	European Securities and Markets Authority
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
MAB	Comitato Market Abuse
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
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
sim	subscriber's identity module (modulo d'identità del sottoscrittore)
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

Acronimi UO dell'Istituto

Valgono quelli in uso (cfr. A6).

A5 – Scheda della CONSOB

Denominazione dell'Ente	CONSOB Commissione Nazionale per le Società e la Borsa
Denominazione dell'Area Organizzativa Omogenea	CONSOB
Codice Identificativo assegnato alla AOO	CONSOB
Nominativo del Responsabile per la tenuta del Protocollo informatico, per la gestione dei flussi documentali e degli archivi	Barbuzzi Gianpaolo Eduardo
Sito internet ufficiale della AOO	www.consob.it
Casella di posta elettronica istituzionale dell'AOO	consob@pec.consob.it
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale	Via Giovanni Battista Martini, 3 - 00198 Roma Telefono (centralino): +39 06 84771 Fax: +39 06 8416703 - +39 06 8417707
Indirizzo completo della sede secondaria operativa di Milano a cui indirizzare l'eventuale corrispondenza convenzionale	Via Broletto, 7 - 20121 Milano Telefono (centralino): +39 02 724201
Data di istituzione della AOO	1974
Data di soppressione della AOO	*vige*

A6 – UO della CONSOB

FIGURE APICALI / DIVISIONI / UFFICI NON COORDINATI	Sigla UO
AVVOCATO GENERALE	AGE
CONSULENZA LEGALE	CLE
DIREZIONE GENERALE	DIR
DIVISIONE AMMINISTRAZIONE	DAM
DIVISIONE CORPORATE GOVERNANCE	DCG
DIVISIONE INFORMAZIONE EMITTENTI	DIE
DIVISIONE INTERMEDIARI	DIN
DIVISIONE ISPETTORATO	DIS
DIVISIONE MERCATI	DME
DIVISIONE STUDI	DST
DIVISIONE STRATEGIE REGOLAMENTARI	DSR
DIVISIONE TUTELA DEL CONSUMATORE	DTC
SEGRETARIATO GENERALE	SEG
UFFICIO ATTIVITÀ PARLAMENTARE E DI GOVERNO	UAP
UFFICIO CONTROLLO INTERNO	UCI
UFFICIO DI PRESIDENZA	UPR
UFFICIO PROGRAMMAZIONE FINANZIARIA E BILANCIO	UPF
UFFICIO RELAZIONI INTERNAZIONALI	URI
UFFICIO SANZIONI AMMINISTRATIVE	USA
UFFICIO DI SEGRETERIA DELLA CAMERA DI CONCILIAZIONE E ARBITRATO	UCA
UFFICIO DI SEGRETERIA DELLA COMMISSIONE	USC
UFFICIO STAMPA	UST
VICE DIRETTORE GENERALE	VDG

UFFICI COORDINATI IN DIVISIONI	Sigla UO
DIVISIONE AMMINISTRAZIONE:	*DAM*
UFFICIO AMMINISTRAZIONE E CONTRATTI – MILANO	AMM
UFFICIO AMMINISTRAZIONE E CONTRATTI – ROMA	AMR
UFFICIO AMMINISTRAZIONE ECONOMICA DEL PERSONALE	AMP
UFFICIO ARCHITETTURE	ARC
UFFICIO GESTIONE RISORSE E FORMAZIONE	GRU
UFFICIO SALUTE E SICUREZZA SUL LAVORO	ASL
UFFICIO RELAZIONI SINDACALI	RES
UFFICIO SVILUPPO E SUPPORTO APPLICAZIONI	VSA

DIVISIONE CORPORATE GOVERNANCE:	*DCG*
UFFICIO CONTROLLI SOCIETARI E TUTELA DIRITTI DEI SOCI	COT
UFFICIO OPA E ASSETTI PROPRIETARI	OPA
UFFICIO VIGILANZA REVISORI LEGALI	REV
DIVISIONE INFORMAZIONE EMITTENTI:	*DIE*
UFFICIO INFORMAZIONI SU OPERAZIONI DI FINANZA STRAORDINARIA	OFS
UFFICIO PROSPETTI EQUITY E IPO	IPO
UFFICIO VIGILANZA INFORMAZIONE EMITTENTI	VIE
DIVISIONE INTERMEDIARI	*DIN*
UFFICIO PROSPETTI NON EQUITY	PNE
UFFICIO VIGILANZA BANCHE E IMPRESE DI ASSICURAZIONE	VIB
UFFICIO VIGILANZA IMPRESE DI INVESTIMENTO	VIN
UFFICIO VIGILANZA INTERMEDIARI-RETE, PROMOTORI E CONSULENTI FINANZIARI	VIP
UFFICIO VIGILANZA SGR E OICR	VGR
DIVISIONE ISPETTORATO	DIS
UFFICIO ACCERTAMENTI ISPETTIVI SU FENOMENI ABUSIVI E ANTIRICICLAGGIO	ABU
UFFICIO ISPEZIONE SU EMITTENTI E REVISORI	ISE
UFFICIO ISPEZIONE SU INTERMEDIARI E MERCATI	ISI
DIVISIONE MERCATI	DME
UFFICIO ABUSI DI MERCATO	ABM
UFFICIO ANALISI QUANTITATIVA E INNOVAZIONE FINANZIARIA	ANQ
UFFICIO AUTOMAZIONE E INTEGRAZIONE PROCESSI DI VIGILANZA MERCATI	APM
UFFICIO GIUDIZI DI RATING E RACCOMANDAZIONI DI INVESTIMENTO	GRI
UFFICIO INFORMAZIONE MERCATI E AGENZIE DI RATING	IME
UFFICIO POST-TRADING	POT
UFFICIO VIGILANZA INFRASTRUTTURE DI MERCATO	VIM
UFFICIO VIGILANZA OPERATIVITÀ MERCATI A PRONTI E DERIVATI	VME
DIVISIONE STUDI	DST
UFFICIO BIBLIOTECA	BIB
UFFICIO PIANIFICAZIONE STRATEGICA	PIA
UFFICIO STATISTICHE	TAT
UFFICIO STUDI ECONOMICI	TEC
UFFICIO STUDI GIURIDICI	TGI
DIVISIONE STRATEGIE REGOLAMENTARI	DSR
UFFICIO ANALISI DI IMPATTO DELLA REGOLAMENTAZIONE	AIR
UFFICIO REGOLAMENTAZIONE	REG

DIVISIONE TUTELA DEL CONSUMATORE	DTC
UFFICIO RELAZIONI CON IL PUBBLICO	REP
UFFICIO CONSUMER PROTECTION	COP
UFFICIO VIGILANZA SU FENOMENI ABUSIVI	VFA

A7 – Elenco PEC

Nelle tabelle seguenti sono riportati tutti gli indirizzi di PEC attivate nell'Istituto e disciplinate nell'ambito del Manuale. L'indirizzo PEC è utilizzato dal sistema DEMACO per l'invio automatico della corrispondenza protocollata in uscita da parte della rispettiva unità organizzativa.

PEC istituzionale e PEC relative alle UO

Indirizzo PEC	Unità organizzativa
consob@pec.consob.it	Direzione generale - Indirizzo istituzionale
seg@pec.consob.it	Segretariato generale
cle@pec.consob.it	Consulenza legale (in uso anche per l'Avvocato generale)
upr@pec.consob.it	Ufficio di presidenza
upf@pec.consob.it	Ufficio programmazione finanziaria e bilancio
uap@pec.consob.it	Ufficio attività parlamentare e di governo
uri@pec.consob.it	Ufficio relazioni internazionali
ust@pec.consob.it	Ufficio stampa
usa@pec.consob.it	Ufficio sanzioni amministrative
usc@pec.consob.it	Ufficio di segreteria della commissione
uci@pec.consob.it	Ufficio controllo interno
uca@pec.consob.it	Ufficio di segreteria della camera di conciliazione e arbitrato[14]
die@pec.consob.it	Divisione informazione emittenti
dcg@pec.consob.it	Divisione corporate governance
dme@pec.consob.it	Divisione mercati
din@pec.consob.it	Divisione intermediari
dis@pec.consob.it	Divisione ispettorato
dst@pec.consob.it	Divisione studi
dam@pec.consob.it	Divisione amministrazione
dsr@pec.consob.it	Divisione strategie regolamentari
dtc@pec.consob.it	Divisione tutela del consumatore

PEC operative

Il sistema gestisce, inoltre, in automatico i seguenti indirizzi PEC per la corrispondenza in entrata, attivati per specifiche finalità "operative" in fase antecedente al 1° luglio 2013.

Indirizzo PEC operativo	Unità organizzativa responsabile
amp@pec.consob.it	Ufficio amministrazione economica del personale
amr@pec.consob.it	Ufficio amministrazione e contratti – Roma
amm@pec.consob.it	Ufficio amministrazione e contratti – Milano
abm@pec.consob.it	Ufficio abusi di mercato
pne@pec.consob.it	Ufficio prodotti non equity
vap@pec.consob.it	Ufficio vigilanza intermediari-rete, promotori e consulenti finanziari
ipo@pec.consob.it	Ufficio prospetti equity e IPO

[14] La *Camera di conciliazione e arbitrato* utilizza per la corrispondenza con l'esterno, per le proprie finalità istituzionali, l'indirizzo PEC: camera@camera-consob.legalmail.it (come riportato in successiva tabella).

PEC funzionali

Sono attivati, infine, i seguenti indirizzi PEC "funzionali" dedicati a specifiche funzioni dell'Istituto, gestite e protocollate nel sistema DEMACO.

Indirizzo PEC funzionale	Attività - Unità organizzativa
sudbond@pec.consob.it	Gestione bond per lo sviluppo – PNE
infobond@pec.consob.it	Informazioni bond – PNE
fondounicogiustizia@pec.consob.it	Fondo Unico Giustizia – Comitato Sequestro e Confisca
contributi@pec.consob.it	Contributi di vigilanza – UPF
malattia@pec.consob.it	Segnalazioni malattia – AMP
gare@pec.consob.it	Gestione corrispondenza di gara – AMR e AMM
consulenzalegale@pec.consob.it	Relazioni formali – Consulenza legale
risorseumane@pec.consob.it	Risorse umane – GRU
vsa@pec.consob.it	Attività di sviluppo software – DAM
portalicrowdfunding@pec.consob.it	Attività di crowdfunding – DIN
autoritatrasparente@pec.consob.it	Attività in materia di Autorità Trasparente – DAM
camera@camera-consob.legalmail.it	Camera di conciliazione e arbitrato – UCA

A8 – 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.

A9 – Loghi, timbri, etichette CONSOB

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

Etichetta di segnatura del protocollo in ingresso CONSOB Prot. 0056830/13 del 01/07/2013	*Segnatura elettronica del protocollo in uscita* Prot. 0045463/14 del 30/05/2014
Logo e indirizzi della busta in uscita CONSOB COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA VIA G.B. MARTINI, 3 00198 ROMA VIA BROLETTO, 7 20121 MILANO	*Logo Delibera ufficiale* CONSOB
Logo per la Comunicazione esterna CONSOB COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA	*Logo per la Comunicazione interna* *(e come seconda pagina nella comunicazione esterna)* CONSOB
Timbro per la distinta di corrispondenza COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA - ROMA	*Timbro di sede con indirizzo* *(ad es. per cartoline A/R)* CONSOB Via G.B. Martini, 3 00188 Roma CONSOB Via Broletto, 7 - MILANO
Timbro per la distinta del corriere RICEVUTO DALLA CONSOB in data.....	
Timbro di "Accettazione"in ingresso CONSOB 19 MAG 2014 ACCETTAZIONE	*Timbro di "Ricevuto" in ingresso* RICEVUTO DALLA CONSOB in data 22 MAG. 2014
Timbro per consegna a mano al Protocollo CONSEGNATO ALLA CONSOB in data..... dal Sig..... RICEVUTO DA	*Timbro per smistamento plico riservato L4* L4

A10 – Titolario di Classificazione CONSOB

CONSOB			
Titolario di classificazione			
Indice di classificazione	Titolo	Indice di classificazione	Classe
01	Organi di governo	01.01	Commissione
		01.02	Presidente
		01.03	Segretario Generale
		01.04	Direttore Generale
		01.05	Vice Direttore Generale
		01.06	Avvocato Generale
		01.07	Funzionari Generali
		01.08	Comitati e Gruppi di lavoro
		01.09	Comitato tecnico
		01.10	Strumenti di coordinamento
		01.11	Collegio dei Revisori dei conti
02	Amministrazione generale	02.01	Legislazione e fonti normative
		02.02	Regolamentazione interna
		02.03	Documentazione organizzativa, funzionale, di processo e di policy
		02.04	Sistema informativo, sicurezza dell'informazione e sistema informatico
		02.05	Protezione dei dati personali
		02.06	Sistema documentale
		02.07	Controlli interni
		02.08	Pianificazione e controllo
		02.09	Studi, analisi e ricerche
		02.10	Banche dati e anagrafiche
03	Vigilanza sugli intermediari	03.01	Gestione Albi ed Elenchi
		03.02	Vigilanza sulla trasparenza e sulla correttezza
		03.03	Vigilanza sugli Organismi
		03.04	Vigilanza sui fenomeni abusivi
		03.05	Gestione delle crisi
		03.06	Vigilanza ispettiva
		03.07	Attività sanzionatoria
04	Vigilanza sui mercati	04.01	Gestione Albi ed Elenchi
		04.02	Vigilanza informativa e sull'integrità dei mercati
		04.03	Vigilanza sul funzionamento e l'organizzazione delle infrastrutture di trading e post-trading
		04.04	Vigilanza regolamentare
		04.05	Vigilanza abusi di mercato
		04.06	Vigilanza ispettiva
		04.07	Attività sanzionatoria
05	Vigilanza sugli emittenti e sulla revisione contabile	05.01	Vigilanza informativa
		05.02	Vigilanza su informazione finanziaria
		05.03	Vigilanza su organi di amministrazione e controllo delle società quotate
		05.04	Controlli di qualità su Società di revisione legale e Revisori legali dei conti
		05.05	Vigilanza su Società di revisione legale e Revisori legali dei conti
		05.06	Accertamento requisiti per emissione titoli assoggettati ad imposta sostitutiva agevolata (c.d. T.R.E.M. bond) e gestione del relativo elenco
		05.07	Vigilanza ispettiva
		05.08	Attività sanzionatoria
		05.09	Gestione elenco emittenti diffusi
06	Vigilanza sulle offerte al pubblico e sull'ammissione a quotazione	06.01	Offerta al pubblico di sottoscrizione e vendita (OPVS, OPS e OPV) e/o ammissione a quotazione
		06.02	Offerte pubbliche di acquisto e scambio (OPAS, OPA, OPSC)
		06.03	Vigilanza sui fenomeni abusivi
		06.04	Vigilanza ispettiva
		06.05	Attività sanzionatoria
07	Attività di regolamentazione	07.01	Supporto alla normativa primaria
		07.02	Normativa secondaria
		07.03	Strumenti interpretativi
		07.04	Verifica dell'impatto della regolamentazione
08	Attività legale	08.01	Contenzioso attivo
		08.02	Contenzioso passivo
		08.03	Recupero spese-crediti da sentenze
		08.04	Consulenze e pareri
09	Rapporti istituzionali e con l'esterno	09.01	Gestione dei rapporti con le istituzioni nazionali e gli organismi esterni nazionali
		09.02	Cooperazione con organismi e istituzioni internazionali
		09.03	Gestione dei rapporti con le istituzioni internazionali
		09.04	Procedimenti di accesso agli atti
		09.05	Esposti
		09.06	Risposte a quesiti e richieste di informazioni
		09.07	Informativa sulle attività istituzionali
		09.08	Gestione contenuti internet
		09.09	Stampa
		09.10	Pubblicazioni
		09.11	Convegni ed eventi
10	Gestione del personale	10.01	Concorsi e selezioni
		10.02	Comandi e distacchi
		10.03	Incarichi
		10.04	Gestione del rapporto di lavoro
		10.05	Valutazione e sviluppo
		10.06	Retribuzione, compensi e rimborsi
		10.07	Adempimenti fiscali, contributivi e assicurativi
		10.08	Trattamento di quiescenza
		10.09	Servizi a domanda individuale
		10.10	Gestione presenze e assenze
		10.11	Relazioni sindacali
		10.12	Salute e sicurezza sul lavoro
		10.13	Procedimenti disciplinari
		10.14	Formazione
11	Gestione delle risorse finanziarie, strumentali e dei servizi	11.01	Programmazione Finanziaria e Bilancio
		11.02	Gestione Contabile - Entrate
		11.03	Gestione Contabile - Spese
		11.04	Gestione ruoli
		11.05	Acquisti di beni, servizi e lavori - Locazioni
		11.06	Gestione beni immobili
		11.07	Gestione beni mobili e mobili registrati
		11.08	Gestione ed esecuzione servizi e forniture particolari
		11.09	Biblioteca
12	Camera di Conciliazione e Arbitrato	12.01	Conciliazione
		12.02	Arbitrato
		12.03	Gestione degli elenchi conciliatori e arbitri
		12.04	Corrispondenza
		12.05	Normativa
13	Oggetti diversi		