BANCA D'ITALIA
EUROSISTEMA

Gestione dell'Informazione

I. PARTE

BANCA D'ITALIA
EUROSISTEMA

MANUALE DI GESTIONE DOCUMENTALE

SOMMARIO

ELENCO DEGLI ACRONIMI

Acronimo	Descrizione
A.R.TE	Procedura Automazione Richieste da Terzi (CR)
ABEF	Procedura Arbitro Bancario e Finanziario
AgID	Agenzia per l'Italia Digitale
AC	Amministrazione Centrale
AOO	Area Organizzativa Omogenea
AS	Area Segretariale - profilo utente "addetto all'Area Segretariale"
AUO	profilo utente "addetto all'Unità Operativa"
CAD	Codice dell'Amministrazione Digitale
CASC	Centro di Assistenza Sociale e Culturale
CD	Capo Dipartimento - profilo utente "Capo Dipartimento"
CDM	Centro Donato Menichella
CP	Centro di Protocollo - profilo utente "addetto al Centro di Protocollo"
CPAC	Centro di protocollo dell'Amministrazione Centrale
CPFIL	Centri di protocollo delle Filiali
CPSPA	Centro di protocollo del Servizio Segreteria particolare del Direttorio e comunicazione
CPUIF	Centro di protocollo dell'Unità di informazione finanziaria
CSAC	Centro di Spedizione dell'AC
CSO	Capo di Struttura Organizzativa - profilo utente "Capo di Struttura Organizzativa"
CSR	Cassa di Sovvenzioni e Risparmio fra il Personale della Banca d'Italia
CUO	Profilo utente "Capo di Unità Operativa"
D.lgs.	Decreto legislativo
DP	Dipartimento
DPCM	Decreto del Presidente Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DSO	Profilo utente "Dirigente di Struttura Organizzativa"
EIEF	Istituto Einaudi per l'Economia e la Finanza
FALDAN	Procedura Falsi & Danneggiati
GEDOC	Divisione Gestione dei documenti del Servizio Gestione dell'Informazione
GES	Servizio Gestione Sistemi Informatici
GIN	Servizio Gestione dell'Informazione
IPA	Indice delle Pubbliche Amministrazioni
IVASS	Istituto per la Vigilanza sulle Assicurazioni
MD	Membro del Direttorio - profilo utente "Membro del Direttorio"
ORG	Servizio Organizzazione
PDR	Punto di ricezione
PEC	Posta Elettronica Certificata
SCDI	Sistema di conservazione dei documenti informatici
SGDD	Sistema di gestione documentale digitale
SIPROS	Sistema Integrato Procedura di Spesa
SIR	Servizio Interno di recapito

Acronimo	Descrizione
SO	Struttura Organizzativa
SVI	Servizio Sviluppo informatico
Testo Unico	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR 28 dicembre 2000, n. 445)
UG	Utente Gestore - profilo utente "addetto all'Utente Gestore"
UGL	Utente Gestore Locale - profilo utente "addetto all'Utente Gestore Locale"
UIF	Unità di Informazione Finanziaria
UO	Unità Operativa

L'elenco completo delle definizioni utilizzate nel *Manuale* è contenuto nel *Glossario*.

1. PRINCIPI GENERALI

1.1. A COSA SERVE IL MANUALE DI GESTIONE DOCUMENTALE

Il *Manuale di gestione documentale* (di seguito, *Manuale*) descrive e disciplina il sistema di gestione informatica dei documenti acquisiti e formati dalla Banca d'Italia (di seguito, Banca).

Il *Manuale* fornisce le istruzioni per il corretto funzionamento e la tenuta del protocollo informatico, la gestione dei flussi documentali, la tenuta degli archivi.

1.2. CHE COSA È UN DOCUMENTO

Un documento[1] è qualunque rappresentazione, comunque formata, di atti (anche destinati a circolare internamente alla Banca), fatti o dati, intelligibili direttamente da un supporto fisico (**documento analogico**) o attraverso un processo di elaborazione elettronica (**documento informatico**).

Sono documenti informatici:

- i documenti direttamente prodotti in formato digitale (ad esempio una e-mail)
- le copie per immagine su supporto informatico (scansioni) di documenti cartacei[2].

1.3. LA GESTIONE DOCUMENTALE

È l'insieme delle attività di trattamento dei documenti finalizzate a garantire la certezza documentale, l'assegnazione alla Struttura competente e l'ordinata conservazione nel tempo del documento.

a) Certezza documentale

Si ha quando sono garantite:

Autenticità (certezza dell'autore - certezza della provenienza). Il documento non può essere disconosciuto

Integrità (completezza e inalterabilità del documento)

Identità (Attributo che caratterizza un documento in modo unico e lo distingue da ogni altro documento).

b) Assegnazione

È il processo che consente di individuare, per ogni documento, la Struttura organizzativa competente (assegnazione per competenza) e, all'interno di questa, assicurarne la presa in carico da parte dell'Unità Operativa responsabile della lavorazione (assegnazione per responsabilità). L'assegnazione deve essere effettuata tempestivamente così come l'eventuale riassegnazione ad altra Struttura nel caso il documento non risulti di competenza dell'assegnatario originario.

Ogni documento deve, altrettanto tempestivamente, essere preso in carico dall'Unità operativa responsabile, che deve eventualmente trasmetterlo a tutte le altre unità organizzative interessate. Il processo di assegnazione si completa con la presa in carico.

c) Ordinata conservazione

---

[1] Non rientrano nella definizione di documento e non sono, quindi, disciplinati dal Manuale: le Gazzette Ufficiali, i bollettini ufficiali e i notiziari della Pubblica Amministrazione, i giornali, le riviste, i libri, gli opuscoli e analoghe fattispecie; i dépliant, il materiale pubblicitario e analoghe fattispecie; le comunicazioni offensive, chiaramente prive di senso compiuto ovvero ripetitive di altre comunicazioni già trasmesse e acquisite dal sistema di gestione documentale. Queste categorie (definite "fattispecie non documentali") non devono essere conferite in archivio.

[2] Non sono da considerare documenti, ai fini della gestione documentale, le stampe cartacee di documenti digitali (ad esempio la stampa del testo di una e-mail).

Tutte le attività che garantiscono la conservazione dei documenti nel tempo e la loro ricerca attraverso le procedure e gli strumenti di classificazione e fascicolazione.

1.4. RIFERIMENTI NORMATIVI

Il *Manuale* rispetta la legislazione in materia di gestione documentale e, in particolare, è conforme ai seguenti testi normativi:

- DPR 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (di seguito, Testo Unico);
- D.lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale (di seguito, CAD);
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici[3];
- DPCM 3 dicembre 2013, Regole tecniche per il protocollo informatico (artt. 2, comma 1; 6; 9; 18, commi 1 e 5; 20; 21.

[3]Le Linee guida dell'Agenzia per l'Italia digitale costituiscono le regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento.

1.5. IL MODELLO ORGANIZZATIVO ADOTTATO DALLA BANCA D'ITALIA. AREA ORGANIZZATIVA OMOGENEA

La Banca si configura come un'unica Area Organizzativa Omogenea (di seguito, AOO)[4] composta da Direttorio, Amministrazione Centrale, Filiali.

1. Direttorio

Il Vertice della Banca è costituito dal Direttorio, di cui fanno parte:

- il Governatore;
- il Direttore Generale
- i Vicedirettori Generali.

2. Amministrazione Centrale

L'Amministrazione centrale è articolata in **Dipartimenti** (di seguito DP)[5] che si compongono di Unità organizzative denominate **Servizi.** L'Unità di Risoluzione e gestione delle crisi, l'Unità di Supervisione e normativa antiriciclaggio, l'Unità Euro digitale, il Servizio Consulenza legale, il Servizio Revisione interna, il Servizio Segreteria particolare del Direttorio e il Servizio Comunicazione sono collocati alle dirette dipendenze del Direttorio.

Le Unità organizzative (di seguito SO) sono a loro volta articolate in **Divisioni** (di seguito, UO)[6].

3. Filiali

L'organizzazione territoriale si articola in Filiali (SO)[7].

Nell'ambito di ciascun DP o SO opera, di norma, una specifica UO (di seguito, "**Area Segretariale**" o AS) con compiti segretariali di gestione e assegnazione per responsabilità della documentazione classificata come **non riservata** alle unità operative.

La Banca ha, inoltre:

- Delegazioni all'estero

e, per specifiche attività, si avvale dei seguenti Enti collaterali:

- Cassa di Sovvenzioni e risparmio fra il personale della Banca d'Italia, di seguito CSR;
- Centro di Assistenza Sociale e Culturale, di seguito CASC;
- Istituto Einaudi per l'Economia e la Finanza, di seguito, EIEF.

[4] Insieme degli uffici che hanno una gestione coordinata e unitaria della documentazione, al fine di svolgere la loro funzione o attività. L'AOO in sostanza è un raggruppamento di unità organizzative della PA che in modo sistematico e coordinato fanno ricorso allo stesso servizio per la gestione del protocollo informatico.
[5] Ai Dipartimenti è preposto un Capo Dipartimento, coadiuvato, di norma, da uno o più Vice Capi Dipartimento.
[6] Nell'ambito delle UO possono essere costituiti Settori; a ciascun Settore è preposto un Titolare.
[7] A ciascuna SO è preposto un elemento con funzioni di Titolare; a queste possono essere assegnati Dirigenti o altro personale in staff, che compongono la Direzione della SO.

Le Delegazioni e gli Enti collaterali non sono inquadrati nell'AOO.

I DP, le SO e le Delegazioni all'estero, con le relative competenze, sono dettagliatamente descritti sul sito Internet della Banca (www.bancaditalia.it).

1.6. LA GESTIONE DOCUMENTALE DELLA BANCA.

1.6.1. I documenti formati o acquisiti dalla Banca

La Banca forma o acquisisce le seguenti tipologie di documenti:

A) Documenti analogici:

a) documenti cartacei con contenuto ufficiale;

b) documenti cartacei con contenuto di rilevanza temporanea (bolle di lavoro e analoghi formulari posti in essere con ditte incaricate di lavori per conto della Banca, comunicazioni di auguri, condoglianze ecc., copie di lavoro, bozze e documentazione di supporto);

c) moduli cartacei ricevuti dall'esterno o a sola rilevanza interna;
d) immagini e video su supporti fisici;
e) telegrammi.

B) Documenti informatici:

a) comunicazioni esterne trasmesse a mezzo posta elettronica certificata (PEC)[8];
b) comunicazioni o documenti interni con caratteristiche informative a rilevanza interna;
c) comunicazioni trasmesse a mezzo posta elettronica ordinaria[9];
d) documenti gestiti attraverso specifiche applicazioni informatiche quali, ad esempio, servizi di trasferimento *file* di grandi dimensioni (*file sharing*), moduli digitali;
e) documenti registrati su supporto rimovibile quali, ad esempio, dischi ottici e *pendrive*[10].

1.6.2. Come si svolge la gestione documentale della Banca

La gestione documentale viene effettuata attraverso:

- il Sistema di gestione documentale digitale (di seguito, **SGDD**), ovvero il sistema informatico per la tenuta del protocollo informatico, la gestione dei flussi documentali e la tenuta degli archivi di cui all'art. 61 del Testo unico;

- altre specifiche modalità previste dal Manuale.

Il SGDD gestisce di norma le seguenti tipologie di documenti

[8] La Banca dispone di una casella PEC cd. "generalista" (bancaditalia@pec.bancaditalia.it) e di caselle PEC di Struttura per ciascun Dipartimento, Servizio o Unità e Filiale. Alcune SO dispongono, inoltre, di caselle PEC cd. "funzionali". Le caselle PEC di Struttura, collegate all'organigramma della Banca, sono create d'ufficio dal Servizio Gestione dell'Informazione (GIN) sentito il Servizio Organizzazione (ORG) e sono associate alla procedura corrispondenza. Le richieste di modifica della configurazione in procedura di una casella PEC devono essere inviate al Servizio Sviluppo informatico (SVI) per competenza e al Servizio GIN per conoscenza (cfr. 3.1.1).

[9] La Banca dispone di una casella cd. "generalista" (email@bancaditalia.it); i dipendenti della Banca dispongono, per esigenze di servizio, di una casella di posta elettronica ordinaria individuale; le SO e le UO dispongono di caselle di posta elettronica ordinaria funzionali (cfr. 3.1.3).

[10] Il Centro di protocollo che riceve un supporto rimovibile allegato a una comunicazione cartacea di **livello inferiore a riservata** ne carica il contenuto nell'applicativo tra gli allegati della comunicazione cartacea (anche in formato compresso, laddove necessario) dopo aver effettuato le previste verifiche di sicurezza sul supporto rimovibile. Il CP conserva la comunicazione cartacea mentre il supporto rimovibile viene trasferito alla Struttura destinataria attraverso il SIR. Del trasferimento del supporto alla Struttura viene inserita annotazione nella scheda documentale.

A) Comunicazioni esterne

- Sono documenti in arrivo e in partenza da e verso soggetti esterni alla Banca:

1. **documenti cartacei** con contenuto ufficiale, compresi quelli prodotti o ricevuti in forma di moduli (fatte salve le eccezioni previste dalle norme interne);
2. **documenti informatici** inviati tramite casella PEC e ricevuti sulle caselle PEC della Banca;
3. **documenti informatici** ricevuti sulla casella di posta elettronica ordinaria generalista che provengono da casella PEC o, se provenienti da casella di posta elettronica ordinaria, sottoscritti con firma qualificata o digitale o per le quali vi sia sufficiente certezza della provenienza[11];
4. **richieste** acquisite tramite le funzionalità rese disponibili dallo "Sportello del Cittadino" (cfr. 1.6, lett. B)d).

B) **Comunicazioni a rilevanza interna** (cfr. 1.6, lett. B)b)

- sono documenti destinati a circolare solo all'interno dalla Banca o indirizzati alle Delegazioni all'estero e agli enti collaterali:

a) **comunicazioni interne**, cioè comunicazioni scambiate tra SO della Banca, nonché con le Delegazioni all'estero e con gli Enti collaterali della Banca;

b) **documenti interni**, di interesse esclusivamente interno alla SO che li forma (appunti, promemoria, verbali, ecc.) e, di norma, non destinati a circolare al di fuori di essa. In tale ambito rientrano anche gli appunti per il Vertice della Banca (appunti per il Direttorio);

c) **comunicazioni ai dipendenti,** cioè comunicazioni destinate direttamente a tutti o alcuni dipendenti.

C) Fattispecie documentali ulteriori

- Sono soggette a registrazione particolare:

a) fatture attive e passive, notifiche del Sistema di interscambio, note di credito e note di debito (gestite anche dalla procedura SIPROS);

b) comunicazioni riguardanti la segreteria dell'Arbitro bancario finanziario (gestite anche dalla procedura ABEF);

c) comunicazioni riguardanti le procedure di gara (gestite attraverso la piattaforma gare telematiche);

d) comunicazioni che accompagnano la consegna di biglietti falsi o danneggiati (gestiti in base a un accordo tra i Servizi interessati).

Non sono gestiti attraverso il SGDD:

I. fattispecie non documentali;

II. documenti cartacei aventi contenuto di rilevanza temporanea (cfr. 1.6, lett. A) b);

III. documenti informatici aventi contenuto di rilevanza temporanea (bolle di lavoro e analoghi

[11] Gli esposti presentati dai cittadini, in considerazione dell'interesse della Banca ad acquisire informazioni utili allo svolgimento delle funzioni di vigilanza, si ritengono, salvo palesi evidenze contrarie, di provenienza certa anche in assenza della sottoscrizione con firma qualificata o digitale.

formulari posti in essere con ditte incaricate di lavori per conto della Banca, comunicazioni di auguri, condoglianze ecc., copie di lavoro);

IV. moduli a sola rilevanza interna (cfr. 1.6, lett. A) c);

V. riproduzioni (cfr. 1.6, lett. A) d);

VI. fattispecie documentali gestite attraverso altre specifiche applicazioni informatiche (cfr. 1.6, lett. B) d), fatta eccezione per quelle di cui al presente paragrafo, lettera C) "Fattispecie documentali ulteriori");

VII. plichi recanti un contrassegno relativo a tematiche di sicurezza nazionale.

Non sono gestiti attraverso il SGDD, fatti salvi i casi previsti dal Manuale:

VIII. documenti informatici scambiati a mezzo di caselle PEC funzionali non associate alla procedura corrispondenza[12] (cfr. 1.6, lett. B), a), 3.1.1, 3.1.3 e 3.3.2 e ss.) [13];

IX. documenti informatici inviati dalla Banca utilizzando caselle di posta elettronica ordinaria (cfr. 1.6, lett. B) c);

X. documenti informatici ricevuti su caselle di posta elettronica ordinaria o sulla casella di posta elettronica ordinaria generalista da caselle di posta elettronica ordinaria e non sottoscritti con firma qualificata o digitale (cfr. 1.6, lett. B) c) e 3.3.8);

XI. telegrammi (cfr. 1.6, lett. A e);

XII. documenti scambiati dagli avvocati della Consulenza Legale nell'ambito dell'attività di gestione del contenzioso della Banca.

[12] Nelle caselle PEC funzionali associate alla procedura corrispondenza, le *mail* in entrata sono protocollate automaticamente.

[13]

2. IL SISTEMA DI GESTIONE DOCUMENTALE DIGITALE

2.1. PREMESSA

I dipendenti sono tenuti a prendere visione di tutte le comunicazioni ricevute, consultando con regolarità la propria casella di posta in arrivo nel SGDD.

2.2. RUOLI E ORARI DI ATTIVAZIONE E DI SERVIZIO

2.2.1. Ruoli

Il **Servizio Gestione dell'informazione** (GIN) è responsabile della gestione amministrativa del SGDD.
Il Responsabile della gestione documentale e della Conservazione dei documenti informatici[14] è il Titolare *pro tempore* del Servizio GIN.

Gestione amministrativa

La Divisione Gestione dei documenti del Servizio GIN (di seguito, GEDOC), in qualità di Unità di gestione (cfr. 2.5.4), supervisiona il corretto funzionamento e l'appropriato utilizzo del SGDD da parte degli utenti e fornisce supporto agli stessi per i problemi di natura amministrativa.

Alla Divisione Archivio Storico del Servizio GIN fanno capo gli aspetti concernenti il piano di classificazione aziendale (cfr. 2.4.1), il Piano di conservazione (o Massimario di selezione e scarto) e la selezione dei documenti da destinare alla conservazione permanente.

Gestione tecnica

I Servizi Sviluppo informatico (di seguito, SVI) e Gestione sistemi informatici (di seguito, GES) sono responsabili della gestione tecnica del SGDD (piattaforma tecnologica, programmi elaborativi e archivi di dati di cui essa si compone), che curano per gli aspetti di competenza e in coordinamento con il Servizio GIN. Il Servizio SVI, in particolare, è la SO responsabile tecnica dell'applicazione informatica a supporto del SGDD.

2.2.2. Orario di attivazione e orario di servizio del SGDD

Il SGDD è operativo continuativamente dalle ore 2,00 alle ore 23,00 in tutti i giorni dell'anno (orario di attivazione).
L'orario di servizio del SGDD, durante il quale è operativo il Service Desk gestito dal Servizio GES, è dalle ore 8,00 alle ore 19,00 di tutti i giorni dell'anno, tranne le giornate di sabato, domenica, Capodanno, Lunedì dell'Angelo, 1° maggio, Natale e S. Stefano.
È operativo un servizio di help-desk per la segnalazione di problematiche di tipo amministrativo e tecnico.

Istruzioni e manuali operativi

Le istruzioni operative per l'utilizzo del SGDD sono contenute nel Sistema di gestione documentale digitale (Procedura ERMES) – Manuale operativo (di seguito, Manuale operativo), disponibile nella Intranet.
Le istruzioni per l'attivazione del servizio di help-desk sono contenute nel documento Sistema di gestione documentale digitale (procedura ERMES) – Istruzioni per la segnalazione di problematiche ai Servizi gestori, disponibile nella Intranet.

[14] Cfr. Manuale di conservazione documentale.

2.3. PROTOCOLLAZIONE

Il sistema di protocollazione è unico[15].
I documenti gestiti attraverso il SGDD sono soggetti alle operazioni di registrazione e segnatura di protocollo.
La **registrazione di protocollo** consiste nella memorizzazione, per ciascun documento, delle informazioni di cui al paragrafo 2.3.1, tra cui gli estremi di protocollo (numero e data di protocollo).
Le informazioni oggetto di registrazione di protocollo di ciascun documento formato o acquisito sono riportate nel **Registro di protocollo**[16].

2.3.1. Informazioni oggetto della registrazione di protocollo

Formano oggetto della registrazione di protocollo le seguenti informazioni:

A. numero sequenziale, univoco e progressivo per anno (numero di protocollo);

B. data di protocollo, attribuita nel momento in cui il documento, in arrivo o in partenza, viene assoggettato a protocollo. Di norma, la data coincide, per i documenti in arrivo, con quella di ricezione; per i documenti in partenza, con quella di spedizione;

C. mittente e destinatario, rispettivamente, per i documenti acquisiti e per quelli formati;

D. oggetto, che esprime in forma sintetica il contenuto del documento, in modo da garantirne l'agevole identificazione rispetto ad altri di analogo argomento[17];

E. estremi del documento ricevuto (data e numero di protocollo) per le comunicazioni esterne in arrivo;

F. indicazione delle SO e delle UO assegnatarie, per competenza o per conoscenza;

G. attributo di riservatezza (cfr. 2.1);

H. indicazione dell'eventuale tipologia di dati personali presenti nel documento (facoltativo);

I. annotazioni (indicazioni facoltative relative al documento);

J. impronta del documento informatico, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata nelle memorie del sistema in forma non modificabile e non accessibile agli utenti.

Non sono modificabili:

[15] Le procedure informatiche SIPROS e ABEF utilizzano sequenze numeriche dedicate ricavate nell'ambito dell'applicazione che supporta il SGDD.
[16] Cfr. Manuale di conservazione documentale.
[17] Fatti salvi i vincoli di riservatezza e tenendo conto delle disposizioni vigenti in materia di protezione dei dati personali e del segreto d'ufficio, l'oggetto va redatto secondo i principi di univocità e uniformità, individuando le parole chiave che esprimono le azioni comunicate nel documento.

- numero di protocollo;
- data di registrazione di protocollo;
- mittente per i documenti ricevuti o, in alternativa, destinatario per i documenti spediti;
- oggetto del documento;
- data e protocollo del documento ricevuto, se disponibili;
- annotazioni;
- per i documenti trasmessi in via telematica, l'impronta del documento informatico.

Le informazioni non modificabili sono annullabili con le modalità previste dall'art. 54 del DPR 445/2000.

La **segnatura di protocollo** consente di individuare ogni documento in modo inequivocabile e comprende:

- numero di protocollo;
- data di protocollo;
- identificazione in forma sintetica dell'amministrazione (Banca d'Italia).

Numero e data di protocollo (estremi di protocollo) sono riportati sulla scheda documentale e attraverso le funzionalità del SGDD direttamente sulla prima pagina del documento o mediante apposizione di un'etichetta sul documento cartaceo.

2.3.2. Annullamento della protocollazione e modifiche della registrazione di protocollo

Il SGDD consente di annullare la protocollazione di un documento secondo le modalità indicate nella procedura riportata in Appendice.
I dati oggetto di annullamento e/o di modifica rimangono comunque memorizzati negli archivi informatici del SGDD.

2.1. ATTRIBUTO DI RISERVATEZZA

2.1.1. Livelli di riservatezza

Le informazioni trattate dalla Banca nell'esercizio delle sue funzioni istituzionali, se non destinate alla pubblicazione, presentano un profilo di riservatezza il cui livello è attribuito sulla base di quanto previsto dalla Circolare n. 276 in relazione agli impatti negativi che la loro diffusione all'esterno potrebbe determinare per l'Istituto anche in conseguenza di violazione dei diritti e delle libertà delle persone fisiche.
A seconda del livello di riservatezza attribuito alle informazioni contenute, ai documenti gestiti attraverso il SGDD è assegnato rispettivamente l'attributo di riservatezza (cfr. Circ. n. 276):

- Alto
- Medio
- Basso

Un documento con riservatezza alta viene contrassegnato come "riservatissimo"
Un documento con riservatezza media viene contrassegnato come "riservato".
L'attributo di riservatezza è assegnato:

a) per le comunicazioni in arrivo dall'esterno, dai Centri di Protocollo (CP), dalle Aree Segretariali (AS) delle Strutture che le ricevono o dall'UO competente per la lavorazione del documento (cfr. 3.2.2, 3.3.2, 3.3.3 e 3.3.5);

b) per le comunicazioni esterne in partenza, le comunicazioni interne e i documenti interni, dalla SO che li predispone.

La variazione dell'attributo di riservatezza viene effettuata secondo quanto previsto nella Circolare n. 276.

2.1.2. Accessibilità ai documenti in relazione all'attributo di riservatezza

I documenti con attributo di riservato e riservatissimo sono conservati crittografati nel SGDD. L'accessibilità a tali documenti è consentita ai soli soggetti specificamente abilitati secondo quanto disciplinato dai paragrafi 3.3.3 e 5.1.3. Le abilitazioni possono essere concesse dai Capi delle SO a singoli dipendenti ovvero a gruppi (c.d. *ad hoc*) individuati per determinate tipologie di documenti.

2.2. ACCESSIBILITÀ AI DOCUMENTI IN RELAZIONE ALLA TIPOLOGIA DEI DATI PERSONALI

Il SGDD consente di indicare la presenza nei documenti di una o più tipologie di dati personali definite nella Circolare n. 257, ossia:

- dati personali
- dati altamente personali
- particolari categorie di dati personali
- dati personali relativi a condanne penali e reati

La possibilità di associare ai documenti l'attributo che individua la presenza di dati personali è consentita a tutti gli utenti.

La facoltà di rimuovere gli attributi che indicano la presenza di una delle tipologie di dati personali è consentita solo agli utenti specificatamente abilitati al trattamento di tale categoria.

Il SGDD consente anche di indicare la presenza di documenti contenenti dati personali nei fascicoli archivistici. In questo caso, l'indicazione si configura solo come un'etichetta indicativa della presenza dei dati personali e non preclude l'accesso al fascicolo.

2.3. ATTRIBUTO DI RISERVATEZZA E PRESENZA DI DATI PERSONALI

Gli impatti negativi per l'Istituto possono essere determinati anche da una violazione di riservatezza di informazioni contenenti dati personali da cui possa derivare un pregiudizio per i diritti e le libertà delle persone.

Ai documenti che contengono:

- particolari categorie di dati personali;
- dati personali relativi a condanne penali e reati

deve essere assegnato attributo di riservatezza pari al massimo a "riservato", ferma restando la valutazione delle Strutture alla luce delle Circolari n. 276 e n. 257.

Se nel documento sono presenti sia dati personali sia dati di altra natura (riguardanti le attività istituzionali della Banca), la cui circolazione indebita può determinare impatti per la Banca, l'attributo di riservatezza del documento tiene conto dell'impatto maggiore fra i due e pertanto potrà essere assegnato un attributo di riservatezza anche **superiore** a "riservato".

Per estendere la visibilità, qualora necessario, a utenti non abilitati a trattare documenti riservati ma autorizzati a trattare queste tipologie di dati personali, le Strutture interessate potranno utilizzare gruppi *ad hoc*.

2.4. CLASSIFICAZIONE E FASCICOLAZIONE

2.4.1. Classificazione

La classificazione, obbligatoria per legge, consiste nell'attribuire al fascicolo archivistico e ai documenti in questo contenuti una codifica su tre livelli (titolo, classe e sottoclasse) selezionata tra quelle contenute nel Titolario (Piano di classificazione).
Nel SGDD la classificazione viene assegnata al documento automaticamente nel momento in cui viene inserito nel fascicolo archivistico (cfr. paragrafo seguente).
Il Servizio GIN comunica alle Strutture le modifiche di volta in volta apportate al Piano di classificazione in base alle funzioni e ai compiti svolti dalla Banca e ne mantiene, anche attraverso le funzioni del SGDD, la storicizzazione per risalire alla classificazione dei vecchi documenti.

2.4.2. Fascicolazione archivistica

Per legge tutti i documenti devono essere inseriti in un fascicolo archivistico.
Il **fascicolo archivistico** è un'aggregazione organizzata di documenti, che evidenzia il legame fra più documenti e il loro contesto di produzione e di esecuzione, facilitandone la ricerca. Il SGDD consente la creazione e gestione di fascicoli archivistici digitali.
Ci sono cinque diversi tipi di fascicolo[18]:

- per affare[19];
- attività[20];
- persona fisica;
- persona giuridica;
- procedimento amministrativo.

Alla conclusione dell'affare o del procedimento, il fascicolo deve essere chiuso; per i fascicoli per attività è prevista la chiusura alla fine di ciascun anno solare.
Per una corretta fascicolazione archivistica dei documenti, gli utenti hanno a disposizione la Guida alla fascicolazione e il Glossario.

2.4.3. Raccolte documentali

Il SGDD consente un'ulteriore modalità di raggruppamento digitale dei documenti: la raccolta

[18] Per maggiori informazioni si veda l'Allegato 5, "I Metadati", delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* dell'AgID.
[19] Il fascicolo "per affare" conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Ha durata circoscritta.
[20] Il fascicolo "per attività" comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice e reiterata, per la quale non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.

documentale[21]. La **raccolta documentale** consente di inserire documenti, anche aventi classificazione differente, oltre che nel pertinente fascicolo archivistico, in una o più ulteriori aggregazioni autonomamente definite dalle Strutture o dai singoli utenti.
L'inserimento dei documenti in una raccolta documentale è obbligatorio per le materie di Vigilanza, per gli inserti[22] e per gli appunti per il Direttorio; negli altri casi è facoltativo (cfr. Manuale operativo e Guida alla fascicolazione).

2.5. PROFILI UTENTE

2.5.1. Generalità

L'operatività nel SGDD è consentita ai soli dipendenti ai quali sia stato assegnato almeno un "profilo utente" all'interno di un'unità organizzativa di appartenenza.
I profili utente e l'assegnazione a un'unità organizzativa garantiscono che ogni utente abbia accesso solo alle funzionalità necessarie per svolgere il proprio lavoro, mantenendo la sicurezza e l'integrità del sistema di gestione documentale
Il profilo utente è costituito dall'insieme delle abilitazioni attribuite a ciascun dipendente per lo svolgimento dei compiti assegnati e in relazione alla posizione funzionale rivestita.
I profili utente si distinguono in:

- profili base (cfr. 2.5.2 e 2.5.3); essi, ad eccezione dei profili AS e CP, sono organizzati in modo gerarchico, ossia ogni profilo include sia le proprie funzionalità specifiche sia quelle dei profili di livello inferiore;

- profili opzionali (cfr. 2.5.4) che forniscono specifiche abilitazioni e consentono l'accesso a particolari funzioni. I profili opzionali sono cumulabili tra loro e con i profili base.

A ciascun profilo utente possono inoltre, essere associate specifiche abilitazioni (opzionali) all'accesso ai documenti sia in relazione all'attributo di riservatezza loro associato sia alla tipologia di dati personali in essi contenuti.

A ciascun soggetto che opera nell'ambito del SGDD sono quindi assegnati:

- un profilo base

- una struttura/unità organizzativa di appartenenza (DP, SO o UO[23])

e possono essere assegnati:

- uno o più profili opzionali in relazione alle attività che deve svolgere (UGL o UG, Firma)

- ulteriori specifiche abilitazioni in base alla tipologia di documenti cui deve accedere (livello di riservatezza, tipologie di dati personali).

Soggetti con il medesimo profilo utente, quindi, possono essere abilitati in maniera diversa all'accesso ai documenti in relazione alle abilitazioni di cui dispongono per accedere ai documenti con un determinato attributo di riservatezza ovvero all'autorizzazione al trattamento delle tipologie di dati personali[24].

---

[21] Già definita "fascicolazione standard" o "complementare".
[22] Vedi glossario.
[23] In merito alla gestione di documenti contenenti particolari categorie di dati o dati giudiziari cfr. la Circolare n. 257/2004, par. 4.1 (Designazione delle persone autorizzate al trattamento).
[24] Nel caso in cui non viene effettuata la designazione esplicita con comunicazione di servizio degli autorizzati al trattamento, tutti gli addetti della Struttura sono abilitati all'accesso a tutte le tipologie di dati personali (Cfr. Cir. n. 257/04, Cap. III, par. 4.1).

I profili utente e le abilitazioni all'accesso ai documenti in relazione sia al livello di riservatezza sia alla tipologia di dati personali sono assegnati dal Titolare della SO, nel rispetto dei livelli fissati dalla normativa interna in materia[25].
I Titolari di ciascuna SO possono altresì inserire le persone in una o più unità organizzative "virtuali"[26], indipendentemente dall'appartenenza a una specifica UO.
Le funzionalità del visto e della firma digitale dei documenti sono esercitate in conformità a quanto previsto dalla normativa interna in materia.

2.5.2. Profili base utenti non direzionali

Addetto all'UO (profilo "AUO")

Il profilo utente degli addetti all'unità operativa (AUO) consente, nell'ambito dell'UO di appartenenza:

- la gestione dei documenti in arrivo (fascicolazione) e la predisposizione, la modifica e il protocollo dei documenti in partenza;
- l'integrazione delle informazioni richieste sul mittente dalle linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici.

Addetto al CP (profilo "CP")

Il profilo utente degli addetti al Centro di Protocollo (CP) consente, nell'ambito delle competenze assegnate al CP (cfr. da 3.2.1 a 3.2.3) e relativamente ai documenti in arrivo alla Banca, di effettuare:

- la registrazione di protocollo di primo livello[27];
- la copia per immagine su supporto informatico;
- l'assegnazione dei documenti alla SO destinataria per competenza e alle eventuali SO destinatarie per conoscenza.

Addetto all'AS (profilo "AS")

Il profilo utente degli addetti all'Area Segretariale (AS) consente, relativamente alle SO rientranti nella competenza di ciascuna unità segretariale (cfr. 3.3.4 e 4.2.3), di:

- gestire i documenti, provenienti dal CP o ricevuti sulla casella PEC di Struttura già sottoposti a registrazione di protocollo di primo livello, assegnandoli per la presa in carico alla UO destinataria per competenza e alle eventuali UO destinatarie per conoscenza;
- integrare le informazioni richieste sul mittente dalle linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici;
- stampare e spedire le comunicazioni esterne in formato cartaceo.

Il profilo AS è assegnato agli elementi appartenenti all'unità segretariale, fermo restando quanto

[25] Cfr Circolari n. 276 e n. 257.
[26] Unità costituite per soddisfare le esigenze gestionali di separazione delle attività di una Struttura o di un'unità organizzativa, senza alcun riferimento all'organigramma effettivo della Banca.
[27] Cfr., paragrafo 3.2.2.

previsto dal paragrafo 2.5.1.

2.5.3. Profili base utenti direzionali

Componenti del Direttorio (profilo "MD")

Il profilo utente assegnato ai membri del Direttorio (MD) consente:

- la visibilità
- il visto
- la firma

di tutti i documenti riguardanti la Banca e le sue Strutture organizzative, centrali e periferiche.
Di norma, inoltre, i componenti del Direttorio sono abilitati ai documenti con qualsiasi attributo di riservatezza e tipologia di dati personali.

Capi dei Dipartimenti (profilo "CD")

Il profilo utente assegnato ai Capi dei Dipartimenti e relativi Vice (CD) consente:

- la visibilità
- il visto
- la firma

di tutti i documenti riguardanti Strutture organizzative del proprio Dipartimento.
Di norma, inoltre, i Capi dei Dipartimenti e i loro Vice sono abilitati ai documenti con qualsiasi attributo di riservatezza.

Titolare di Struttura organizzativa (profilo "CSO")

I Titolari di Struttura Organizzativa e i relativi Vice hanno il profilo utente CSO e il profilo "Firma" che consentono:

- la visibilità
- il visto
- la firma

di tutti i documenti riguardanti la propria SO.
I Titolari di Struttura e i relativi Vice sono di norma abilitati a gestire i documenti con qualsiasi attributo di riservatezza e ad assegnarli per competenza alle UO del Servizio.
Il Titolare della SO può assegnare il profilo CSO, di norma, al proprio sostituto, stabilendo contestualmente il livello di abilitazione per la visibilità dei documenti in ragione del diverso attributo di riservatezza.
Il profilo CSO della Struttura è assegnato agli ispettori incaricati di accertamenti di revisione interna per il periodo di durata dell'incarico.

Dirigente di SO (profilo "DSO")

Il profilo utente Dirigente di Struttura Operativa (DSO) consente la visibilità dei documenti riguardanti la SO di appartenenza.

Al profilo è associata l'abilitazione al visto e alla firma dei documenti, da esercitarsi nel rispetto delle competenze e delle deleghe ricevute.
Il Titolare della SO assegna il profilo DSO, di norma, ai Dirigenti e altro personale in staff della SO e stabilisce il livello di abilitazione per la visibilità dei documenti in relazione al loro livello di riservatezza.

Titolare di UO (profilo "CUO")

Il profilo utente dei Titolari di Unità Operative (CUO) consente di accedere a tutti i documenti nella visibilità (in lettura o scrittura) della UO di appartenenza[28].
Il profilo CUO consente di valutare e quindi prendere in carico o rifiutare[29] i documenti e gli atti assegnati per competenza all'UO.
Al profilo è associata l'abilitazione al visto e alla firma dei documenti, da esercitarsi nel rispetto delle competenze e delle deleghe ricevute.

2.5.4. Profili opzionali

Utente Gestore (profilo "UG")

Il profilo Utente Gestore[30] (UG) consente di svolgere le attività di carattere generale connesse con la gestione amministrativa del SGDD quali l'annullamento dei protocolli, l'aggiornamento dell'organigramma, la configurazione degli utenti.

Utente Gestore locale (profilo "UGL")

Il profilo Utente Gestore locale (UGL) consente di amministrare i profili utente nell'ambito delle SO di competenza. É, di norma, assegnato a elementi appartenenti all'unità segretariale, fermo restando quanto previsto dal paragrafo 2.5.1.

Assistente di direzione (profilo "AD")

Il profilo Assistente di direzione (AD) è assegnato, di norma, agli elementi che svolgono compiti di supporto segretariale agli Utenti direzionali[31] (componenti del Direttorio, CD, titolari di SO e di UO).

2.6. DIGITALIZZAZIONE DI DOCUMENTI CARTACEI. MEMORIZZAZIONE DEI TESTI E DELLE INFORMAZIONI OGGETTO DELLA REGISTRAZIONE DI PROTOCOLLO

2.6.1. Digitalizzazione di documenti cartacei

I documenti cartacei sia in arrivo sia in partenza, compresi gli allegati ufficiali, sono riprodotti in copia per immagine su supporto informatico mediante scansione in formato non modificabile.

L'immagine acquisita mediante scansione deve essere:

- conforme all'originale;
- integra;
- completa.

[28] Il profilo "CUO" è assegnato al Titolare dell'UO, al sostituto e, con l'accordo del Capo Servizio, agli elementi che coadiuvano direttamente il Titolare nella gestione dell'UO, stabilendo contestualmente il livello di abilitazione.
[29] Cfr. 3.3.5 (le UO accettano la responsabilità del documento o dell'atto o, se non di competenza, la rifiutano prontamente).
[30] Il profilo "UG" è assegnato dai rispettivi Titolari di SO a elementi appartenenti alla Divisione GEDOC, ai Servizi SVI e GES.
[31] Ciascun Assistente di direzione può essere assistente di uno o più utenti direzionali. Il profilo consente di svolgere le medesime funzioni del profilo assegnato all'utente direzionale, a eccezione di visto e firma dei documenti.

Non è ammessa la digitalizzazione parziale (ad esempio la copia del solo documento e non anche degli eventuali allegati) o di testi recanti cancellature apposte dal destinatario.

La responsabilità della conformità delle copie per immagine dei documenti cartacei è attribuita a elementi incaricati dai titolari delle Strutture presso la quale è effettuata la copia.

I Titolari predispongono gli opportuni presidi volti a garantire la corretta esecuzione delle operazioni di copia e sono responsabili dell'esecuzione della verifica su base campionaria della corretta digitalizzazione dei documenti in arrivo.

2.6.2. Memorizzazione e accessibilità ai testi e alle informazioni oggetto della registrazione di protocollo.

Il SGDD memorizza i testi dei documenti, sia cartacei sia informatici, e le relative informazioni oggetto della registrazione di protocollo.

L'accesso ai dati è consentito agli utenti del SGDD in base al profilo e all'ufficio loro assegnato.

2.7. SICUREZZA DEI DATI, DEI SISTEMI E DELLE INFRASTRUTTURE. PIANO PER LA CONTINUITÀ OPERATIVA E PIANO DI *DISASTER RECOVERY*. REGISTRO DI PROTOCOLLO DI EMERGENZA

2.7.1. Sicurezza dei dati, dei sistemi e delle infrastrutture

Il SGDD è realizzato in conformità delle regole tecniche di cui al CAD, art. 51. In particolare:

A) la sicurezza fisica è garantita dai presidi previsti per l'accesso agli stabili e ai locali della Banca dove sono collocati gli elaboratori;

B) la sicurezza logica dei dati è garantita da un'unica utenza privilegiata residente nel SGDD;

C) l'accesso alle informazioni in base ai singoli profili utente è gestito automaticamente dal SGDD;

D) i documenti con attributo di riservato e riservatissimo sono crittografati nel SGDD. Il passaggio dei documenti dal sistema fisico di archiviazione ai posti di lavoro attraverso la rete aziendale è sempre crittografato;

E) i documenti informatici da inviare all'esterno dell'Istituto (con PEC o posta ibrida: v. infra) sono trasmessi sempre ed esclusivamente su canali sicuri;

F) i documenti informatici provenienti dall'esterno dell'Istituto sono filtrati attraverso antivirus;

G) il passaggio dei dati dal SGDD al Sistema di conservazione dei documenti informatici è governato utilizzando un canale cifrato e i dati contenuti nel Sistema sono accessibili esclusivamente dal Responsabile del Sistema stesso o dalle persone da lui delegate. Il SGDD registra in uno specifico archivio (*log*) tutti gli accessi in lettura.

2.7.2. Piano di continuità operativa e piano di *disaster recovery*

Il piano di continuità operativa e il piano di *disaster recovery* del SGDD sono parte dei rispettivi piani della Banca a livello aziendale.
In particolare:

- tutti gli archivi fisici e i sistemi sono duplicati per garantire continuità di servizio all'applicazione;

- sono attivate giornalmente procedure di *back-up* sia dei dati, sia dei documenti.

2.7.3. Registro di protocollo di emergenza

Qualora per cause tecniche non sia possibile utilizzare il SGDD, il Capo del Servizio GIN in qualità di Responsabile del servizio di protocollo informatico autorizza l'utilizzo del Registro di protocollo di emergenza, regolato in allegato (cfr. Appendice, Sezione II).
Una volta ripristinata la disponibilità del SGDD, i documenti già protocollati "in emergenza" sono sottoposti al protocollo ordinario, annotando sui documenti stessi gli estremi del protocollo di emergenza[32].

3. DOCUMENTI IN ARRIVO DALL'ESTERNO

3.1. RICEZIONE E TRATTAMENTO DEI DOCUMENTI

3.1.1. Ricezione dei documenti analogici e informatici

I **documenti analogici** in arrivo dall'esterno indirizzati alla Banca d'Italia, a Strutture interne all'Istituto, a Organi statutari della Banca d'Italia o a suoi componenti oppure a dipendenti presso la sede di lavoro sono ricevuti e gestiti presso i Punti di ricezione (PDR).

Punti di ricezione:

A) **Via Nazionale n. 91, 00184 Roma** per i documenti indirizzati ai componenti del Direttorio, ai CD, alle SO dell'AC e alla Filiale di Roma CDM; il PDR è gestito dalla Divisione GEDOC. Lo sportello "accettazione" della documentazione è aperto tutti i giorni feriali (sabato escluso) dalle ore 9,00 alle ore 15,00 (nelle giornate semifestive dalle ore 9,00 alle ore 12,00);

B) **Largo Bastia, n. 35, 00181 Roma** per i documenti indirizzati all'UIF; il PDR competente per la ricezione è l'unità segretariale dell'UIF;

C) **Via dei Mille, 52, 00185 Roma** per i pignoramenti ivi notificati presso il Servizio TES;

D) le **Sedi di Filiale**, agli indirizzi indicati sul sito Internet della Banca, per i documenti di rispettiva competenza; i PDR competenti sono le unità segretariali di ciascuna Filiale.

I **documenti informatici** assumono rilevanza ufficiale se inviati da un mittente esterno:

- tramite casella PEC;
- tramite casella di posta elettronica ordinaria, purché sottoscritti con firma digitale o qualificata o corredati da copia di un valido documento d'identità, oppure sia comunque possibile accertare la fonte di provenienza

e **ricevuti** su:

- caselle di posta gestite dal Centro di protocollo dell'Amministrazione Centrale (CPAC)**:**
    - bancaditalia@pec.bancaditalia.it (casella PEC generalista);

[32] Il Registro del protocollo di emergenza e la copia di cui al Testo unico, artt. 61, c. 3, lett. e) e 63 vengono conservati per dieci anni a cura del Servizio GIN in luoghi sicuri differenti.

- email@bancaditalia.it (casella di posta elettronica ordinaria generalista);

- casella PEC dedicata alla ricezione di atti, comunicata al Ministero della Giustizia e pubblicata sul ReGIndE;

- caselle PEC di Struttura gestite dai DP o dalle SO[33];

- caselle PEC funzionali associate alla procedura.

I documenti inviati alle caselle di posta elettronica non devono superare la dimensione di 100 *megabyte*, non devono contenere *spam*[34] e devono essere in uno dei formati utilizzati e accettati:

- documenti Office (doc, docx, pps, ppsx, ppt, pptx, xls, xlsx);

- documenti OpenOffice (ODG, ODP, ODS, ODT);

- documenti in Portable Document Format (PDF);

- *email* (MSG, EML);

- documenti firmati con firma CAdES (P7M);

- immagini (JPG, JPEG, TIF, TIFF, PNG, GIF, BMP, SVG);

- documenti di testo (CSV, TXT, RTF);

- archivi ZIP;

- XML.

L'utilizzo di formati diversi da quelli elencati non garantisce l'accettazione del documento inviato. Per la valutazione di accettazione di formati diversi, si terrà conto di:

- informazioni contenute in "raccomandazione per la lettura" dell'allegato 2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti;

- caratteristiche di sicurezza e consultabilità;

- possibilità di riversamento nel sistema di conservazione.

Non saranno in alcun modo accettate comunicazioni contenenti *link* a *repository* esterni dai quali scaricare i documenti.

La Banca non assume l'obbligo di accettare documenti inviati a indirizzi fisici o di posta elettronica diversi da quelli indicati sul proprio sito *web* o sull'Indice delle Pubbliche Amministrazioni (IPA).

Le SO che hanno sede in uffici della Banca che non sono PDR possono decidere, per particolari esigenze, di disporre la ricezione dei documenti analogici in arrivo da parte delle portinerie degli edifici. In questi casi devono trasmettere, di regola attraverso il Servizio interno di recapito (di seguito SIR)[35] nella giornata di ricezione o, comunque, con la massima tempestività:

[33] Gli indirizzi delle caselle PEC della Banca sono indicati sul sito internet www.bancaditalia.it.
[34] Le caselle di posta elettronica della Banca sono tutelate da un filtro *antispamming*.
[35] Detto anche "servizio di bolgetta".

I. al competente CP, i documenti gestiti dal SGDD;
II. direttamente all'unità segretariale della SO destinataria i documenti non gestiti attraverso il SGDD e le fattispecie analogiche non documentali.

È fatto divieto ai dipendenti di dare il recapito del posto di lavoro per la ricezione di plichi personali di qualsiasi contenuto. Il personale addetto al CP non accetta raccomandate personali e atti giudiziari indirizzati a persone fisiche se dalla busta della raccomandata o dell'atto non si evinca che il documento contenuto è inequivocabilmente legato alla posizione ricoperta o alla funzione svolta in Banca d'Italia.
Non sono considerati personali i plichi recanti la dizione "alla cortese attenzione di... ", "a …, Titolare di..." o simili.

3.1.2. Trattamento dei documenti analogici

I documenti analogici vengono consegnati alla Banca:

E) dal **vettore di posta**, secondo le modalità concordate.

- I plichi vengono ricevuti:
  - senza particolari formalità, se spediti con modalità ordinaria;
  - previo riscontro, se spediti con modalità cd. "registrata"[36];

F) tramite **consegna a mano** nei giorni, negli orari e secondo le modalità indicate da ciascun PDR. I PDR annotano giornalmente, in ordine cronologico, gli estremi dei plichi così ricevuti su un Registro di sportello.

I Registri di sportello devono essere custoditi per un anno e quindi distrutti informalmente.

Su richiesta del consegnatario, il PDR rilascia ricevuta del plico, senza accertamento del contenuto, con l'indicazione del giorno di consegna.

Sui plichi che contengono, secondo quanto sugli stessi riportati, domande di partecipazione a gare di appalto, il PDR appone immediatamente l'indicazione del giorno e dell'ora di ricezione, mediante timbro orodatario.

I plichi ricevuti dalla Banca vengono consegnati chiusi dai PDR ai competenti CP con modalità fissate dalle SO di appartenenza. Fanno eccezione i plichi indirizzati:

- ai componenti del Direttorio o ai Capi Dipartimento o loro Vice, da trasmettere chiusi, in giornata, alle rispettive segreterie, previa apposizione di firma per ricevuta su modulo cartaceo acquisito agli atti, dell'incaricato del ritiro;

- specificamente a Strutture di Banca recanti l'indicazione "stampe" o il cui contenuto verosimilmente non rientra tra le fattispecie gestite dal SGDD, da trasmettere chiusi alla competente unità segretariale;

- alla Filiale di Roma CDM, da trasmettere chiusi all'unità segretariale della Filiale medesima.

3.1.3. Trattamento dei documenti informatici

Ricezione e gestione dei documenti

[36] Il riscontro viene effettuato per ogni singolo plico mediante la verifica del numero identificativo del codice a barre con la corrispondente distinta di accompagnamento.

La gestione dei documenti ricevuti sulle caselle di posta elettronica è effettuata nei giorni lavorativi durante il normale orario di ufficio.

I documenti **devono** essere sottoposti a protocollazione e a registrazione di protocollo di primo livello se sono inviati da un mittente esterno tramite:

- casella PEC;
- casella di posta elettronica ordinaria e sottoscritti con firma digitale o qualificata o corredati da copia di un valido documento d'identità oppure quando sia comunque possibile accertare la fonte di provenienza.

I documenti informatici ricevuti sulle caselle PEC associate al SGDD sono sottoposti a protocollazione automatica.

I documenti informatici ricevuti sulla casella di posta elettronica ordinaria generalista gestita dal CPAC non sono di norma sottoposti a protocollazione e a registrazione di protocollo di primo livello, salvo che nei casi sopra indicati o su indicazione della SO competente[37].

I documenti informatici ricevuti sulle caselle convenzionali, funzionali, gestite dalle SO o su quelle individuali non sono sottoposti a protocollazione e a registrazione di protocollo ma sono gestiti dagli intestatari delle caselle senza particolari formalità, secondo i criteri stabiliti dal Titolare della SO.

Se necessario, possono essere acquisiti agli atti della Banca:

- allegandoli a un documento interno predisposto nel SGDD;
- richiedendone la protocollazione al competente CP;
- utilizzando le specifiche procedure di protocollazione semiautomatica (per le Strutture che ne hanno la disponibilità).

La protocollazione deve riguardare il messaggio elettronico ricevuto[38]. Le riproduzioni a stampa di documenti informatici non hanno natura di documento cartaceo e, quindi, non possono in nessun caso essere sottoposti a protocollazione.

Assegnazione dei documenti

I documenti pervenuti sulle caselle PEC gestite dal CPAC sono da questo assegnati e inviati alla Struttura organizzativa competente in via esclusiva oppure che ne ha la competenza in misura prevalente ai sensi del Regolamento generale della Banca d'Italia.

I documenti pervenuti sulle caselle PEC delle Strutture sono assegnati direttamente alle Strutture stesse.

All'interno della Struttura assegnataria i documenti sono tempestivamente assegnati all'Unità organizzativa competente per la lavorazione.

Nel caso i documenti siano stati erroneamente assegnati o non siano di competenza (esclusiva o prevalente) della Struttura ricevente, questi devono essere immediatamente riassegnati alla SO competente se nota o, in alternativa, restituiti al CPAC tramite le apposite funzionalità presenti nel

[37] Il CPAC inoltra alla casella funzionale ordinaria della Segreteria della SO il documento per la sua valutazione.
[38] Il *file* da protocollare sarà il messaggio originale ricevuto salvato in formato .msg

SGDD di restituzione del documento al CP e di riassegnazione ad altra Struttura. Nel caso l'errata assegnazione abbia generato una conoscenza impropria di dati personali, si farà riferimento alle previsioni della Circolare n. 257 (Disposizioni in materia di trattamento dei dati personali).

Inserimento dei dati di protocollazione

Il CPAC, l'Area Segretariale della Struttura assegnataria e l'Unità organizzativa competente che prende in carico il documento protocollato, se sono a conoscenza dell'informazione, devono inserire nel SGDD:

- livello di riservatezza;
- segnalazione della presenza di dati personali;
- ulteriori metadati necessari ai fini della conservazione del documento.

L'Area Segretariale che gestisce i documenti in arrivo sulla casella PEC assegnata alla Struttura governa il successivo processo di assegnazione per competenza dei documenti alle Unità organizzative facenti capo alla Struttura assegnataria.

I documenti informatici ricevuti sulle caselle PEC di Struttura:

A) se provenienti da caselle PEC, sono automaticamente sottoposti a protocollazione e a registrazione di protocollo di primo livello;

B) se provenienti da caselle di posta elettronica ordinaria, non sono di norma accettati dalla casella PEC destinataria e, qualora, per particolari esigenze, questa sia abilitata alla loro ricezione, non sono sottoposti a protocollazione e a registrazione di protocollo di primo livello ma sono reindirizzati automaticamente alla competente casella ordinaria funzionale dell'AS della SO assegnataria.

Messaggi PEC incagliati ("sospesi")

Quando la procedura per cause tecniche non riesce a protocollare in automatico un messaggio PEC, esso resta "sospeso" (o "incagliato") e deve essere gestito manualmente dal CP competente tramite l'apposita funzione della procedura.

La protocollazione manuale dei messaggi PEC "sospesi" deve essere effettuata almeno giornalmente[39], anche qualora i messaggi "sospesi" contengano informazioni considerate non rilevanti ai fini della gestione degli atti di competenza (ad esempio, notifiche di consegna).

> In ogni caso i CP non sono tenuti a protocollare o a inoltrare documenti evidentemente stravaganti, palesemente privi di fondamento, rientranti nella categoria dello *spamming* o analoghe fattispecie. I messaggi "sospesi" che rientrano tra quelli da non protocollare vanno quindi eliminati.

3.2. CENTRI DI PROTOCOLLO E LORO ATTIVITÀ

3.2.1. Centri di protocollo

Sono costituiti i seguenti Centri di protocollo (di seguito, CP):

[39] Istruzioni sulla gestione dei messaggi sospesi sono disponibili nella sezione FAQ della pagina intranet di GEDOC https://intranetbi.bancaditalia.it/group/site_1_974_987/gestione-dei-documenti

A) Centro di protocollo dell'Amministrazione Centrale (CPAC), gestito dalla Divisione gestione dei documenti di GIN.

Competente per la gestione, assegnazione e inoltro dei:

- documenti cartacei da assegnare ai Dipartimenti e alle SO centrali;
- documenti informatici ricevuti sulla casella PEC generalista e le altre caselle gestite.

B) Centro di protocollo del Servizio Segreteria particolare del Direttorio e comunicazione (CPSPA), per i documenti di competenza dei componenti del Direttorio;

C) Centro di protocollo dell'Unità di informazione finanziaria (CPUIF), per i documenti di propria competenza;

D) Centri di protocollo delle Filiali (CPFIL), per i documenti di rispettiva competenza; le funzioni dei CPFIL sono svolte, di norma, dalle unità segretariali di ciascuna Filiale.

3.2.2. Competenze dei CP: procedura ordinaria

I CP aprono i plichi ricevuti dal PDR, con l'eccezione di quelli:

- contenenti domande di partecipazione a gare di appalto;
- recanti la dizione "riservato", "riservatissimo" o di natura simile quali ad esempio quelli indirizzati a persona fisica;
- inviati ai componenti del Direttorio o ai Funzionari Generali;
- provenienti da mittenti segnalati per iscritto al Servizio GIN dalle altre Strutture, in casi particolari e per esigenze motivate;
  - contenenti valori sospetti di falsità;
  - recanti un contrassegno relativo a tematiche di sicurezza nazionale.

I CP:

- trasmettono all'unità segretariale della competente SO, senza aprirli né protocollarli, i documenti che non sono gestiti attraverso il SGDD e le fattispecie non documentali (senza distinta di accompagnamento);
- protocollano manualmente i documenti che rientrano tra le fattispecie gestite dal SGDD, inclusi quelli ricevuti sulla casella di posta elettronica ordinaria che le SO richiedano di protocollare, nonché i plichi da non aprire in quanto riservati o riservatissimi.

I CP effettuano la **registrazione di protocollo di primo livello** inserendo le seguenti informazioni:

- mittente;
- oggetto;
- estremi di protocollo del documento ricevuto (se indicati);
- indicazione della SO assegnataria per competenza;

- indicazione della natura del documento ovvero se documento o "atto notificato alla Banca d'Italia";

- livello di riservatezza;

- indicazione dell'eventuale presenza e tipologia di dati personali (se rilevabili).

Per i soli documenti cartacei, una volta ultimata la fase di inserimento dati i CP stampano l'etichetta recante gli estremi di protocollo del documento e la applicano sulla prima pagina del documento o sul plico "da non aprire" ai sensi del presente paragrafo.

I CP effettuano la digitalizzazione dei documenti cartacei ai sensi di quanto indicato nel paragrafo 2.6.1 e acquisiscono il documento informatico da protocollare nel SGDD, associandolo alla scheda documentale. I documenti protocollati e digitalizzati con attributo di riservatezza diverso da riservato e riservatissimo sono inoltrati, con l'avvio del processo di assegnazione, tramite la specifica funzione del SGDD alle AS delle SO assegnatarie. I documenti con attributo di riservatezza riservato o riservatissimo sono inoltrati direttamente all'ufficio del Capo della Struttura.

I documenti contenuti in plichi non recanti specifici livelli di riservatezza che invece, per il loro contenuto, appaiono immediatamente e inequivocabilmente almeno di livello riservato, sono trasmessi, unitamente ai plichi di origine, alla competente unità segretariale in una busta chiusa dopo la registrazione di protocollo di primo livello. Sulla busta e nel SGDD il CP appone annotazione di tale circostanza.

Analogo trattamento è previsto per le domande di partecipazione a bandi di gara contenute in plichi non recanti la relativa dizione.

Le attività necessarie alla digitalizzazione e trasmissione dei documenti sono svolte attraverso le specifiche funzionalità del SGDD, che consentono l'inoltro dei documenti in visibilità, con notifica o senza notifica, alle SO, alle UO o a singoli dipendenti.

I documenti cartacei originali per i quali è stata effettuata la digitalizzazione nel SGDD sono custoditi dai rispettivi CP per anno, in ordine di numero di protocollo. Fanno eccezione i documenti cartacei originali trattati dal CPSPA, che sono trasmessi alle SO assegnatarie.

Per giustificati motivi, le SO possono acquisire dal competente CP documenti analogici originali ad esse assegnati; di tale circostanza il CP fa menzione nel campo "annotazioni".

Sono fatte salve le eccezioni di cui al successivo paragrafo.

3.2.3. Competenze dei CP: casi particolari

Alcune tipologie documentali presentano particolarità tali da richiedere un trattamento specifico:

A) Documenti cartacei che dopo il protocollo e la scansione devono essere sempre inviati ai Servizi di competenza tramite il servizio interno di recapito (SIR, cfr. 5.5)

   a) contratti sottoscritti;
   b) crediti documentari;
   c) dichiarazioni di tassazione in paesi esteri;
   d) fidejussioni;
   e) alcune tipologie di atti notificati alla Banca (v. *infra*).

B) Documenti cartacei non scansionabili, per i quali i CP scansionano la sola lettera di trasmissione

   a) documenti rilegati, indipendentemente dal numero di pagine e tipologia di rilegatura, al

fine di non alterarne l'integrità;
b) documenti particolarmente voluminosi;
c) documenti di formato diverso da A4, A3 e B4;
d) documenti ai quali sono allegati elementi non scansionabili (ad es. planimetrie);
e) documenti riservati e riservatissimi;
f) gare, da trattare come i documenti riservati (da trasmettere in busta chiusa apponendo il protocollo sulla busta).

Non vengono sottoposti a scansione tutti i documenti cartacei particolarmente voluminosi, ad esempio domande di acquisto di partecipazioni (che di regola pervengono con allegati voluminosi e di vario genere), pubblicazioni, indagini statistiche sul credito, chiavi di autenticazione.
I documenti non scansionati devono essere inviati al Servizio di destinazione con modalità tracciata, che garantisca l'avvenuta ricezione e l'individuazione certa della data di ricezione e del soggetto/Struttura ricevente.
Le conferme di ricezione devono essere custodite per almeno sei mesi.
Qualora la scansione non sia stata effettuata dal CP, il Servizio destinatario dovrà scansionare il documento, se possibile, e mantenere l'originale cartaceo ai propri atti.

C) Documenti da non assoggettare al protocollo

Tutte le comunicazioni palesemente stravaganti o prive di fondamento sia in formato cartaceo, sia in formato elettronico, devono essere trattenute presso il CP e distrutte informalmente entro 30 giorni. Eventuali casi dubbi dovranno essere sottoposti alla valutazione della Direzione.
In tutti gli altri casi in cui il trattamento del documento presenti delle particolarità, deve esserne fatta menzione nel campo "annotazioni" della scheda documentale.

D) Atti notificati alla Banca d'Italia

I CP ricevono e gestiscono gli atti notificati alla Banca d'Italia, i quali, per la delicatezza della materia trattata, sono soggetti a un trattamento specifico[40].
Gli atti notificati alla Banca si distinguono in:

- atti giudiziari[41], di competenza del Servizio Consulenza legale (CSL);
- atti che riguardano procedimenti esecutivi in cui la Banca è coinvolta quale terzo pignorato. L'atto deve essere assegnato in base alle indicazioni previste dalle Circolari n. 310/20 e n. 317/22;
- atti tributari, di competenza del Servizio Assistenza e consulenza fiscale (ACF);
- i restanti atti che non rientrano nelle tipologie sopra elencate.

Attraverso le funzioni del SGDD, l'addetto al CP dovrà corredare i metadati del documento in fase di protocollazione/protocollato, scegliendo dal menu a tendina "Tipo di documento" tra i valori:

a) "Atto giudiziario di competenza CSL"
b) "Procedura esecutiva contro dip./pens. BI", di competenza del Servizio Gestione del personale (GEP)
c) "Procedura esecutiva contro ADER", "Procedura esecutiva contro PA" e "Procedura esecutiva contro privati", di competenza del Servizio Tesoreria (TES)
d) "Atti tributari", di competenza del Servizio ACF

[40] Per gli aspetti operativi legati all'assegnazione di questi atti si rimanda all'Appendice (Sezione I).
[41] Riguardano il contenzioso nei confronti della Banca: sono relativi a procedimenti penali e civili di cognizione, anche sommaria, amministrativi e contabili.

e) "Altri atti giudiziari": altri atti giudiziari notificati non rientranti tra quelli precedenti.

Per le lettere a), b), c), d) è prevista la valorizzazione automatica della Struttura assegnataria (metadato "Assegnato a") non appena avvenuta la selezione.
Per gli atti di competenza di GEP il CP imposta l'attributo di riservatezza "riservato".

3.2.4. Modalità di trasmissione dai CP alle unità segretariali

I documenti e gli atti notificati alla Banca d'Italia gestiti attraverso il SGDD sono inoltrati in formato elettronico alle AS delle SO assegnatarie.

I documenti non gestiti attraverso il SGDD (cfr. 3.1.3) e le fattispecie non documentali sono trasmessi alle unità segretariali senza distinte di accompagnamento.

Il CPAC e il CPSPA effettuano la trasmissione attraverso il SIR.

3.3. INCOMBENZE DELLE SO. REGISTRAZIONE DI PROTOCOLLO DI SECONDO E TERZO LIVELLO.

3.3.1. A Assegnazione dei documenti non gestiti attraverso il SGDD e fattispecie non documentali

Le unità segretariali assegnano prontamente i documenti ricevuti che non sono gestiti attraverso il SGDD e le fattispecie non documentali, ricevute dai PDR e dai CP, alla competente UO, d'intesa con i rispettivi Titolari e secondo le modalità operative definite dal Titolare della SO.

3.3.2. Assegnazione dei documenti non riservati gestiti attraverso il SGDD

Il Titolare della SO fornisce alle AS le indicazioni sulla gestione dei documenti cartacei e informatici.

Le AS sottopongono in visione a quest'ultimo e/o ai Dirigenti della SO i documenti cartacei gestiti attraverso il SGDD per i quali non è stata effettuata la digitalizzazione del documento cartaceo e i plichi chiusi contenenti domande di partecipazione a gare di appalto.

Le AS assegnano alla UO competente i documenti e i plichi e inoltrano, attraverso le specifiche funzionalità del SGDD, i relativi estremi di protocollo e le ulteriori informazioni oggetto della registrazione di protocollo di primo livello per la successiva presa in carico.

Le AS ricevono, attraverso le specifiche funzioni del SGDD, i documenti non riservati assegnati dal CP ovvero i documenti ricevuti sulla casella PEC di Struttura.

Le AS assegnano prontamente i documenti, in via digitale, alla competente UO, modificando, se del caso, il livello di riservatezza e le categorie di dati personali presenti nel documento. I Titolari di SO e i Dirigenti di SO ricevono la visibilità senza notifica dei documenti assegnati alla struttura.

Nel caso in cui la competenza ricada su più unità operative, l'AS assegnerà per responsabilità il documento a una UO secondo il principio di prevalenza, inoltrando con notifica la scheda documentale alle ulteriori unità cointeressate.

Nel caso in cui i documenti ricevuti non prevedano lo svolgimento di un'attività sul documento da parte di una specifica UO, le AS interrompono il processo di assegnazione e procedono alla gestione del documento dandone visibilità alle UO o agli utenti o alle unità organizzative comunque interessate.

Le AS restituiscono prontamente, tramite l'apposita funzionalità del SGDD, i documenti non correttamente assegnati alle Strutture. L'azione di "rifiuto" e restituzione del documento al CP deve essere opportunamente motivata. Laddove possibile, per facilitare la successiva riassegnazione da parte del CP, deve essere data indicazione della corretta Struttura di assegnazione. Le AS, se del caso, possono procedere direttamente alla riassegnazione ad altra Struttura della documentazione erroneamente ricevuta tramite la specifica funzione disponibile nel SGDD.

Le AS devono segnalare al CP l'errata qualificazione del documento nel caso questo sia, in realtà, un atto giudiziario notificato alla Banca d'Italia o, viceversa, l'errata qualificazione dell'atto nel caso questo sia un documento generico. L'utilizzo dell'apposita funzione presente nel SGDD comporta la restituzione del documento al CP, che provvede alla modifica della qualifica e alla pronta riassegnazione del documento/atto. In questo caso le Strutture non devono operare la riassegnazione diretta.

3.3.3. Assegnazione dei documenti con livello di riservatezza elevato gestiti attraverso il SGDD

I documenti classificati come riservato o riservatissimo assegnati alla Struttura dal CP o pervenuti sulla casella PEC della Struttura sono ricevuti nel SGDD dal Titolare della SO attraverso un'attività dedicata.

I documenti protocollati dal CP inseriti in plichi chiusi recanti la dizione "riservato" o "riservatissimo" sono consegnati immediatamente dalle unità segretariali al Titolare della SO.

Il Titolare della SO fornisce all'AS l'indicazione del livello di riservatezza se diverso da quello già apposto dal CP.

L'AS procede alla digitalizzazione della documentazione cartacea, ove possibile.

Il Titolare della SO o chi opera in suo conto cura l'assegnazione per competenza della documentazione alla competente UO; può decidere di bloccare il processo di assegnazione all'UO competente attraverso la specifica funzione del SGDD e gestire il documento in modo diverso, inoltrandone la visibilità a utenti o strutture specifiche.

3.3.4. Documenti gestiti attraverso il SGDD: registrazione di protocollo di secondo livello

L'inoltro da parte delle AS alle UO degli estremi di protocollo e delle informazioni oggetto della registrazione di protocollo di primo livello costituisce l'attività di registrazione di protocollo di secondo livello.

3.3.5. Competenze delle UO e registrazione di protocollo di terzo livello

Per i documenti gestiti attraverso il SGDD, le UO devono accettare o rifiutare prontamente (se non di competenza) la responsabilità del documento o dell'atto. In caso di rifiuto il documento/atto torna nella disponibilità dell'area segretariale.

Il documento o l'atto assegnato per competenza all'UO viene esaminato e preso in carico dal Capo dell'UO o da un suo incaricato. Con la presa in carico l'UO assume la responsabilità della lavorazione del documento/atto e la responsabilità del completamento della registrazione di protocollo.

Il Titolare dell'UO, nel caso il documento non sia di competenza della sua UO, rifiuta[42] la presa in carico fornendone i motivi nell'apposito campo che si attiva al momento del rifiuto. In questo caso il documento ritorna all'AS per la successiva assegnazione a UO della Struttura ovvero per la restituzione del documento al CP, ovvero per la riassegnazione diretta ad altra struttura.

Nel caso il documento o atto sia stato erroneamente accettato[43] per responsabilità dalla UO o, a ulteriore esame, risulti non di competenza della UO che lo ha accettato, la UO dovrà prontamente segnalarlo attraverso annotazione sulla scheda documentale e di trasmetterlo per la lavorazione attraverso le funzionalità del SGDD alla UO o alla Struttura effettivamente competente. Se la struttura competente non dovesse essere nota, è possibile inoltrarlo al CPAC.

[42] Le UO accettano la responsabilità del documento o dell'atto o, se non di competenza, la rifiutano prontamente.

[43] Nel caso l'errata assegnazione abbia generato una conoscenza impropria di dati personali, si farà riferimento alle previsioni della Circolare n. 257 (Disposizioni in materia di trattamento dei dati personali).

Una volta accettato il documento, le UO lo classificano e inseriscono in un fascicolo archivistico (**registrazione di protocollo di terzo livello**) ed effettuano, se necessario, la modifica del livello di riservatezza.

Per i documenti ricevuti su supporto rimovibile, le UO verificano se siano leggibili attraverso i sistemi e le applicazioni in uso in Banca. In caso contrario, ne danno pronta informativa al mittente, restituendogli il supporto.

Nel caso in cui il documento venga posto in visibilità o notificato in cassetta postale a più unità operative, le operazioni di registrazione di protocollo di terzo livello devono essere effettuate dalla UO che accetta il documento per competenza.

3.3.6. Documenti gestiti dal SGDD: digitalizzazione del documento

Le AS e le UO effettuano la digitalizzazione dei documenti che non sono stati digitalizzati dal CP, sulla base delle indicazioni fornite dal Titolare della SO. Gli originali cartacei restano conservati a cura della SO.

3.3.7. Modifica di assegnazione dei documenti

Le AS sono tenute a restituire al CP tempestivamente i documenti e gli atti erroneamente assegnati alla SO tramite un'azione di rifiuto, indicando nelle motivazioni la SO competente, se nota.

In caso di restituzione da parte delle UO, le AS possono assegnare il documento per competenza a un'altra delle altre UO della SO di appartenenza[44] ovvero direttamente ad altra struttura dell'AC o della rete periferica.

Per i documenti e atti assegnati, le AS monitorano, attraverso le funzionalità dedicate del SGDD, la tempestiva presa in carico per competenza da parte delle UO.

3.3.8. Certezza documentale

I documenti analogici hanno l'efficacia probatoria prevista dalla normativa in relazione alle loro modalità di formazione e di sottoscrizione.

I documenti informatici assumono rilevanza ufficiale per la Banca se:

- ricevuti sulle caselle PEC generalista o di Struttura o sulla casella di posta elettronica ordinaria generalista (cfr. 3.1.1):

  a) redatti utilizzando formati "statici", senza macro e/o contenuti eseguibili;

  b) ove trasmessi da Pubbliche Amministrazioni, ricorrano le condizioni di cui al CAD, art. 47;

  c) ove trasmessi da soggetti diversi da Pubbliche Amministrazioni, siano inviati da caselle PEC (anche se privi di firma elettronica e non corredati da copia di valido documento di riconoscimento) oppure da caselle di posta elettronica ordinaria purché sottoscritti con firma qualificata o digitale o corredati da copia di valido documento di riconoscimento;

- ricevuti sulle caselle PEC funzionali (cfr. 3.1.1).

I documenti informatici ricevuti sulle caselle di posta elettronica ordinaria diverse dalla generalista non assumono rilevanza ufficiale per la Banca.

[44] Qualora l'errata assegnazione abbia generato una conoscenza impropria di dati personali, si farà riferimento alle previsioni della Circolare n. 257 (*Disposizioni in materia di trattamento dei dati personali*).

4. DOCUMENTI IN PARTENZA VERSO L'ESTERNO

4.1. PREDISPOSIZIONE, APPROVAZIONE, SOTTOSCRIZIONE E PROTOCOLLAZIONE DEI DOCUMENTI GESTITI ATTRAVERSO IL SGDD

4.1.1. Predisposizione

I documenti destinati a soggetti esterni alla Banca sono predisposti come documenti informatici, attraverso le funzionalità del SGDD, dalle UO competenti (profili utente CUO e AUO). La predisposizione di un documento comprende, oltre alla stesura del testo, l'inserimento delle informazioni oggetto di registrazione di protocollo (cfr. 2.3.1).

Nella fase di predisposizione, i documenti possono essere corredati sia da allegati "ufficiali" sia da documentazione "di supporto" (cd. allegati "non ufficiali"). Gli allegati ufficiali sono gestiti in tutte le fasi del processo insieme al documento di riferimento, che viene protocollato nel Registro Ufficiale, e sono inviati al destinatario; successivamente, confluiscono nel sistema di conservazione a norma e restano quindi disponibili con le stesse modalità previste per il documento a cui sono collegati. Gli allegati di supporto, in relazione alla loro natura di documentazione utile solo nella fase di istruttoria e priva di valore ufficiale, rimangono associati, invece, al solo documento di predisposizione, non vengono inviati al destinatario e non confluiscono nel sistema di conservazione a norma.

Laddove sussista l'esigenza di conservare a norma anche la documentazione di supporto, è possibile inserirla come allegato ufficiale di un documento interno (cfr. 5.3.1), indicando nell'oggetto gli estremi del documento a cui fa riferimento (che potrà eventualmente essere anch'esso aggiunto come collegamento). Il documento interno deve essere inserito nello stesso fascicolo del documento di riferimento e quindi protocollato.

Gli allegati possono avere diversi formati. Di preferenza devono essere utilizzati i seguenti:

- documenti Office (doc, docx, pps, ppsx, ppt, pptx, xls, xlsx);
- documenti OpenOffice (ODG, ODP, ODS, ODT);
- documenti in Portable Document Format (PDF);
- email (MSG, EML);
- documenti con firma CAdES (P7M);
- immagini (JPG, JPEG, TIF, TIFF, PNG, GIF, BMP, SVG);
- documenti di testo (CSV, TXT, RTF);
- archivi ZIP e RAR;
- XML.

Per gli appunti al Direttorio gli allegati devono essere necessariamente in formato PDF.

Alcuni formati sono inibiti a priori dal SGDD. Comunque prima di utilizzare formati diversi da quelli sopra indicati occorre tenere conto di:

- indicazioni contenute nella "Raccomandazione per la scrittura" dell'allegato 2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti;

- caratteristiche di sicurezza del formato;
- possibilità di accettazione e consultazione da parte del destinatario della comunicazione;
- possibilità tecniche di portabilità del formato dell'allegato in uno dei formati accettati dal sistema di conservazione (cfr. Manuale di conservazione).

Le comunicazioni che eccezionalmente, sulla base delle valutazioni della SO mittente, debbano essere inviate in formato cartaceo (ad es. lettere di cortesia) devono essere predisposte nel numero di esemplari corrispondente ai destinatari. Per finalità di conservazione, deve essere effettuata a cura dell'unità segretariale una copia per immagine in formato non modificabile, che viene acquisita tramite scansione nel SGDD.

Il documento è automaticamente visibile e modificabile da tutti gli utenti appartenenti alla UO predisponente abilitati al livello di riservatezza attribuito al documento e al trattamento di dati personali, ove presenti. Tali utenti, previa autorizzazione del Titolare della UO, possono estendere la visibilità e la modificabilità dei documenti a elementi di altre UO in possesso delle abilitazioni necessarie, nel rispetto di quanto disposto dalla Circolare n. 276.

All'atto dell'attribuzione della caratteristica di "riservatissimo", il SGDD presenterà di *default* una data convenzionale, dopo la quale il documento perderà automaticamente tale caratteristica per assumere quella di "riservato". Questa data è modificabile dagli utenti abilitati a tale funzione[45].

4.1.2. Lettere automatiche

La funzionalità "lettere automatiche" consente di gestire le comunicazioni prodotte da specifiche procedure. L'utilizzo e la modifica della funzionalità devono essere chiesti ai Servizi GIN e SVI dalle SO che hanno in gestione le procedure.

Le UO dispongono di funzionalità per l'annullamento della protocollazione analoghe a quelle previste per i documenti gestiti secondo le modalità ordinarie (cfr. 4.1.6).

4.1.3. Approvazione

L'approvazione consiste nell'apposizione del visto attraverso le funzionalità del SGDD da parte dei competenti livelli gerarchici (Titolare dell'UO, Dirigenti o altro personale in *staff*, Titolare della SO, Capo Dipartimento).

4.1.4. Sottoscrizione

Le competenze in materia di sottoscrizione dei documenti sono disciplinate dalla Circolare n. 287 (Poteri e responsabilità di gestione e di rappresentanza).

Il documento è sottoscritto con firma digitale o con sottoscrizione autografa a seconda della sua natura di documento elettronico o cartaceo. In entrambi i casi, il documento ha valenza probatoria di scrittura privata non autenticata.

4.1.5. Protocollazione

Il documento viene protocollato al termine dell'iter di approvazione e sottoscrizione, di norma dall'UO che lo ha predisposto. Dopo la protocollazione il documento non è più modificabile.

4.1.6. Annullamento della protocollazione

[45] Secondo la Circolare n. 276, le informazioni devono essere "declassificate" una volta che si riduca o cessi l'esigenza di riservatezza.

La protocollazione dei documenti cartacei o informatici può essere annullata secondo quanto previsto dalle linee guida AgID (cfr. anche Appendice I.III del presente Manuale).

L'annullamento della protocollazione viene chiesto attraverso le funzioni del SGDD dal Titolare dell'UO assegnataria o da un dipendente appartenente alla UO con profilo CUO e deve essere approvato dall'UG.

Gli estremi del protocollo annullato restano memorizzati nel SGDD.

4.2. CANALI DI SPEDIZIONE

4.2.1. Canali di spedizione informatici e tradizionali

I documenti in partenza verso l'esterno possono essere spediti attraverso i seguenti canali:

A) informatici:

   a) caselle PEC;
   b) servizio di posta ibrida, effettuato da un *provider* esterno, che riceve un flusso informatico attraverso le funzionalità del SGDD e cura la riproduzione dei documenti in formato cartaceo, l'imbustamento e il recapito a destinazione;

B) tradizionali:

   a) servizio postale, reso da vettori individuati dalla Banca;
   b) servizio di recapito diretto tramite incaricato della Banca.

4.2.2. Documenti da inviare tramite i canali di spedizione informatici

Sono inviati:

A) tramite caselle PEC, i documenti informatici (cfr. 4.1.1) che non superino la dimensione di 100 *megabyte*[46] indirizzati a destinatari esterni che dispongono di una casella PEC[47]. L'invio è effettuato a cura dell'UO competente attraverso le funzionalità del SGDD. Le Strutture che intendano effettuare invii di un documento a un numero di destinatari superiore a 500 devono contattare preventivamente il Servizio GIN all'indirizzo mail GIN.GestioneDocumenti@bancaditalia.it per concordare le modalità e la data dell'invio delle comunicazioni[48];

C) tramite servizio di posta ibrida, i documenti informatici (cfr. 4.1.1) indirizzati a destinatari esterni che non dispongono di una casella PEC. L'invio è effettuato a cura dell'UO competente attraverso le funzionalità del SGDD. Esigenze di spedizione di documenti particolarmente voluminosi e/o indirizzati a una numerosa platea di destinatari devono essere comunicate con congruo anticipo al Servizio GIN, che valuta modalità alternative di spedizione e informa eventualmente il *provider* esterno.

   Non possono essere inviati tramite servizio di posta ibrida i documenti:

   a) che abbiano caratteristica di riservato o riservatissimo o natura di provvedimenti o atti

[46] La dimensione di ciascun documento viene calcolata moltiplicandola per il numero di destinatari: ad es. un documento di dimensioni pari a 10 *megabyte* inviato a cinque destinatari "pesa" 50 *megabyte*.
[47] Compresi i documenti riservati e riservatissimi e i documenti aventi natura di provvedimenti o atti procedimentali. La caratteristica di riservatezza limita l'accessibilità ai documenti ai soli soggetti specificamente abilitati nel SGDD, ma ovviamente non garantisce la presenza di analoghi presidi presso il destinatario.
[48] Nel caso di invii massivi di PEC si può determinare un flusso di comunicazioni superiore alla capacità dell'SGDD, con conseguenti rallentamenti.

procedimentali, fatte salve specifiche eccezioni stabilite dalla Banca[49];

b) prodotti dalla Banca nella sua veste di Tesoreria per conto dello Stato (di seguito, documenti di Tesoreria).

4.2.3. Documenti da inviare tramite i canali di spedizione tradizionali

Sono inviati tramite i canali di spedizione tradizionale, secondo quanto disciplinato nel paragrafo 4.3:

A) le riproduzioni in formato cartaceo di documenti informatici, recanti la firma per attestazione di conformità agli originali digitali, qualora questi ultimi non possano essere spediti attraverso canali informatici. Tali riproduzioni, in numero pari ai destinatari e recanti in automatico gli estremi di protocollo, sono curate, di norma, dalla competente AS. L'attestazione di conformità al documento originale firmato digitalmente viene apposta dal personale di Banca a ciò autorizzato;

B) i documenti predisposti eccezionalmente in forma cartacea (cfr. 4.1.1), tipicamente su carta di rispetto. Ciascuno di essi deve recare l'etichetta che riporta gli estremi di protocollo; prima dell'invio, deve esserne effettuata copia per immagine mediante scansione a cura, di norma, della competente AS;

C) i documenti analogici rientranti nelle fattispecie non gestite dal SGDD nonché le fattispecie cartacee non documentali.

È escluso il ricorso ai canali di spedizione tradizionali per il recapito di fattispecie diverse da quelle indicate.

In base a quanto previsto dall'art. 47, comma 1, del CAD lo scambio di documenti tra le pubbliche amministrazioni avviene esclusivamente mediante l'utilizzo della posta elettronica o in cooperazione applicativa[50].

4.3. SPEDIZIONE ATTRAVERSO I CANALI TRADIZIONALI: DISPOSIZIONI DI CARATTERE GENERALE

4.3.1. Imbustamento e confezionamento

Tutti i documenti devono essere avviati a spedizione chiusi nelle buste intestate in uso in Banca. I documenti che non possono essere chiusi in tali buste devono essere confezionati in involucri chiusi, sui quali deve essere evidenziata in modo chiaro la provenienza dalla Banca.

In ogni caso il confezionamento deve essere effettuato nel rispetto delle regole concordate con i vettori di cui al 4.2.1, lett. B) a) per l'accettazione dei plichi da spedire (dimensioni, peso, ecc.).

4.3.2. Modalità di svolgimento del servizio di spedizione

I plichi da inviare a destinazione vengono ritirati presso il Centro di spedizione dell'AC (cfr. 4.4.1 e 4.4.3) o presso ciascuna Filiale a cura del vettore di cui al 4.2.1, lett. B) b)[51].

4.3.3. Norme particolari per il servizio di spedizione dei documenti di Tesoreria

I costi di spedizione dei documenti di Tesoreria sono a carico del Ministero competente.

Le modalità di svolgimento del servizio e i tempi di consegna sono comunicati dal Servizio Comunicazione.

---

[49] Ad es. comunicazioni in esito a istanze di accesso ai dati della Centrale dei rischi prodotte automaticamente dalla procedura A.R.TE.

[50] Il comma 1-bis dell'art. 47 prevede che l'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.

[51] Le modalità di svolgimento del servizio di spedizione, i tempi di consegna e le tariffe sono comunicati dal Servizio Comunicazione.

4.3.4. Recapito diretto tramite incaricato della Banca

Le Filiali provvedono al recapito diretto tramite proprio incaricato sulla base delle indicazioni fornite dal Titolare.

Il recapito della documentazione dell'AC è regolato dal 4.4.2.

4.3.5. Competenze delle SO

Le Filiali curano le incombenze descritte dal par. 4.3.1 al par. 4.3.4.

Le SO dell'AC curano le incombenze descritte al par. 4.3.1, di norma tramite l'unità segretariale. La spedizione è curata dal Centro di spedizione dell'AC costituito nell'ambito della Divisione Editoria e stampa del Servizio Comunicazione (cfr. 4.4.1 e 4.4.2).

4.4. SPEDIZIONE ATTRAVERSO I CANALI TRADIZIONALI: CENTRO DI SPEDIZIONE DELL'AC

4.4.1. Documentazione da inviare tramite servizio postale

La documentazione in partenza verso l'esterno deve essere imbustata dalle SO mittenti in conformità di quanto previsto al 4.3.1. I plichi devono recare l'indicazione della SO mittente e l'indirizzo completo del destinatario. I plichi devono essere trasmessi al Centro di spedizione dell'AC (di seguito, CSAC) in bolgette sigillate di colore rosso e accompagnati da distinte in duplice esemplare, recanti l'intestazione della SO e la firma del Titolare dell'unità segretariale, riferite alle seguenti modalità di spedizione:

A) ordinaria[52];

B) raccomandata;

C) raccomandata A/R;

D) assicurata convenzionale A/R.

Le distinte riferite alla documentazione da inviare secondo le modalità di cui alla lett. A) devono indicare il numero complessivo di buste da spedire; quelle relative alle lett. B), C) e D) devono contenere l'elenco delle singole buste da spedire.

Il recapito della documentazione dalle SO al CSAC avviene attraverso il SIR (cfr. da 5.5).

Il CSAC, dopo aver verificato l'integrità dei sigilli delle bolgette, le apre e, controllata la regolarità degli imbustamenti, redige i documenti accompagnatori e li consegna all'incaricato del recapito.

I plichi confezionati in maniera difforme da quanto previsto dal 4.3.1 non possono essere avviati a spedizione e sono restituiti alla competente unità segretariale.

Il CSAC trattiene un esemplare delle distinte e restituisce all'unità segretariale il secondo esemplare, timbrato per ricevuta dei plichi. Queste distinte sono conservate per almeno un anno e, quindi, distrutte informalmente.

Le modalità e i tempi di consegna dal CSAC ai vettori sono definiti dal Servizio Comunicazione. Eventuali esigenze di invio con tempi e modalità diversi da quelli ordinari devono essere rappresentate con congruo anticipo con mail dalla casella funzionale della SO alla casella funzionale COM.Spedizioni@bancaditalia.it.

4.4.2. Documentazione avente carattere di urgenza da consegnare direttamente al destinatario

[52] Per i plichi inviati con modalità "posta ordinaria" non è possibile tracciare l'avvenuta consegna.

Le SO ubicate in Roma o nel Centro Donato Menichella in Frascati (CDM) possono richiedere la consegna diretta a destinazione di documenti nei casi e con le modalità di seguito specificati:

- il servizio può essere richiesto per la consegna di plichi chiusi, di peso non superiore a 2 kg., a destinatari in Roma entro il Grande Raccordo Anulare, esclusivamente in casi di estrema urgenza e se la SO non possa effettuare la consegna con proprio personale;

- la richiesta deve essere presentata entro le ore 16,00 delle giornate lavorative dal lunedì al venerdì, con il massimo anticipo possibile, con mail dalla casella funzionale della SO alla casella funzionale COM.Spedizioni@bancaditalia.it. Nella richiesta deve essere precisato: l'indirizzo dove il plico deve essere ritirato, il nominativo e il contatto telefonico dell'incaricato della consegna al vettore; l'indirizzo, il nominativo e, ove possibile, il contatto telefonico del destinatario;

- ove la SO mittente intenda acquisire una firma di ricezione da parte del destinatario, deve corredare il plico con modulo di ricevuta, che sarà restituito dal CSAC tramite il SIR in occasione del primo utile giro di staffetta (cfr.5.6);

- il ritiro e la consegna del plico sono effettuati, di norma, entro tre ore.

4.4.3. Casi particolari

Il CSAC cura la spedizione della documentazione prodotta dalla CSR, dal CASC e dall'EIEF sulla base delle specifiche convenzioni stipulate tra tali enti e la Banca. Le modalità di trasmissione della documentazione sono analoghe a quelle previste per la documentazione delle SO dell'AC.

Il Servizio GES e il Servizio Immobili curano direttamente la spedizione di documentazione di loro competenza mediante i vettori individuati dalla Banca.

5. COMUNICAZIONI A RILEVANZA INTERNA

5.1. COMUNICAZIONI INTERNE GESTITE ATTRAVERSO IL SGDD

5.1.1. Definizione

Le comunicazioni interne sono quelle scambiate tramite SGDD tra le SO della Banca e con le Delegazioni all'estero, con la CSR e il CASC.

Sono realizzate esclusivamente in formato digitale e sono trasmesse attraverso le funzionalità del SGDD. Gli allegati non gestibili in formato digitale sono trasmessi in formato analogico mediante il SIR o i canali di spedizione tradizionali. L'invio degli allegati in formato analogico deve essere specificato nel testo della comunicazione.

5.1.2. Comunicazioni interne in partenza

Le modalità di predisposizione, approvazione, sottoscrizione e protocollazione delle comunicazioni interne sono le stesse previste per i documenti informatici in partenza verso l'esterno.

5.1.3. Comunicazioni interne in arrivo

Le comunicazioni interne in arrivo sono identificate da:

- segnatura di protocollo;
- classificazione;
- fascicolazione archivistica;
- livello di riservatezza;

- indicazione delle tipologie di dati personali contenuti nel documento.

Tali informazioni sono inserite dalla SO mittente.

La scheda documentale contenente le informazioni oggetto di registrazione di protocollo e i documenti sono inviati automaticamente ai Responsabili della SO e alla relativa AS (nel caso di documenti che non ricoprano un livello di riservatezza corrispondente al livello riservato o riservatissimo).

L'AS o i Responsabili della SO assegnano il documento alla competente UO.

I testi delle comunicazioni interne sono accessibili ai soli soggetti abilitati a seconda del livello di riservatezza attribuito al documento dalla SO mittente.

L'accesso è consentito ai soli soggetti cui viene estesa la visibilità del documento e abilitati al corrispondente livello di riservatezza. L'estensione della visibilità è autorizzata secondo quanto previsto dalla Circolare 276.

La visibilità dei documenti può essere estesa a gruppi *ad hoc* costituiti, su iniziativa del Capo della SO, per la trattazione di specifici affari. L'inserimento nel gruppo *ad hoc* consente la visibilità del documento anche a un membro non abilitato ai riservati o riservatissimi.

5.1.4. Comunicazioni ai dipendenti

Sono comunicazioni destinate direttamente a tutti o alcuni dipendenti e riguardano fatti e circostanze di loro interesse. Tali comunicazioni sono predisposte dalla SO mittente e sono ricevute dai destinatari direttamente nella propria casella di posta del SGDD senza l'intermediazione delle unità di segreteria. La pubblicazione sul SGDD garantisce adeguata informativa.
L'adeguata informativa ai dipendenti in distacco o assenti per lunghi periodi viene effettuata dalle unità con compiti segretariali.

Resta impregiudicato il ricorso a diverse modalità determinate ex lege per specifiche comunicazioni e a ulteriori tipologie di informativa (per es., e-mail o raccomandata A/R) ritenute necessarie a fronte di rilevanti profili di rischio legale.

5.2. COMUNICAZIONI TIPIZZATE E LETTERE AUTOMATICHE GESTITE ATTRAVERSO IL SGDD

5.2.1. Comunicazioni tipizzate

Sono comunicazioni tipizzate le comunicazioni interne aventi contenuto standardizzato e indirizzate a uno o più destinatari predefiniti. Tali comunicazioni sono predisposte dalla SO mittente attraverso le funzionalità del SGDD.

5.2.2. Lettere automatiche

Le lettere automatiche destinate a SO sono gestite secondo le medesime funzionalità previste per le lettere automatiche destinate a soggetti esterni alla Banca (cfr. 4.1.2).

5.3. DOCUMENTI INTERNI GESTITI ATTRAVERSO IL SGDD

5.3.1. Definizione e modalità di gestione

Sono documenti interni quelli di interesse esclusivamente interno alla SO che li forma (appunti, promemoria, verbali, ecc.) e, di norma, non destinati a circolare al di fuori di essa. Rientrano in questa categoria anche gli appunti per il Direttorio.

I documenti interni sono gestiti attraverso il SGDD secondo modalità analoghe a quelle previste per i documenti informatici in partenza verso l'esterno.

5.3.2. Appunti per il Direttorio

Sono documenti interni predisposti dalle SO e indirizzati ai componenti del Direttorio per le decisioni o per informativa. Gli allegati devono essere soltanto in formato PDF.

Gli appunti al Direttorio devono essere sottoscritti digitalmente dal CSO e dal CD competenti e, una volta protocollati dalla struttura proponente, sono inoltrati automaticamente attraverso le funzioni del SGDD al Servizio Segreteria particolare del Direttorio (SPA).

Il Servizio SPA inoltra i documenti all'esame dei singoli membri del Direttorio ovvero, ove richiesto, in seduta collegiale. La conclusione del processo di valutazione crea il documento del Registro ufficiale che contiene la valutazione, i commenti e le annotazioni dei membri del Direttorio.

5.4. TIPOLOGIE DOCUMENTALI NON GESTITE ATTRAVERSO IL SGDD:

5.4.1. Moduli a rilevanza interna

I moduli analogici a rilevanza interna sono elencati nel *Piano di conservazione*; quelli informatici sono gestiti nell'ambito delle applicazioni informatiche della Banca.

5.4.2. Altre fattispecie documentali elaborate nell'ambito di applicazioni informatiche

Le fattispecie documentali elaborate nell'ambito di applicazioni informatiche della Banca sono gestite al di fuori del SGDD, fatto salvo quanto previsto dal 1.6.2 C), secondo modalità che ne garantiscono la certezza documentale, l'assegnazione, l'ordinata conservazione e, ove del caso, la conoscenza della controparte.

5.4.3. Trasmissione di documentazione riservata e riservatissima

Tutta la documentazione classificata come riservata o riservatissima che non passa attraverso il SGDD può essere trasmessa con l'applicazione dei presidi previsti dalla Circolare n. 276. È possibile richiedere chiavi di cifratura anche per le caselle funzionali di posta elettronica[53].

In casi eccezionali e sotto la responsabilità del mittente sarà possibile inviare documentazione cartacea attraverso plichi recanti l'indicazione "riservatissimo".

5.4.4. Documenti informatici scambiati a mezzo posta elettronica ordinaria

I documenti informatici scambiati all'interno della Banca a mezzo posta elettronica ordinaria non sono gestiti attraverso il SGDD.

Le comunicazioni interne a carattere ricorrente e che non presentano particolare rilevanza sotto il profilo documentale devono essere scambiate esclusivamente attraverso le caselle funzionali di posta elettronica ordinaria. Tra queste rientrano, a titolo esemplificativo: le richieste di abilitazioni informatiche, *badge* e tesserini identificativi, interventi di manutenzione.

Considerato che le mail sono memorizzate dal sistema aziendale di posta elettronica per un periodo di tempo limitato, le SO mittenti e destinatarie individuano modalità idonee per la loro conservazione, qualora necessaria.

5.5. SERVIZIO INTERNO DI RECAPITO DELLA DOCUMENTAZIONE ANALOGICA TRA LE SO DELL'AREA ROMANA (SIR)

5.5.1. Ambito di operatività del servizio interno di recapito

Il SIR è un servizio gestito dalla Divisione GEDOC ed effettuato da una ditta esterna, che cura il recapito tra le seguenti strutture dell'Area romana:

[53] Cfr. parte VI "Manuale di posta elettronica".

- SO ubicate in Roma o al CDM;
- Enti collaterali della Banca (CSR, CASC ed EIEF);
- Istituto per la Vigilanza sulle Assicurazioni (IVASS) in via del Quirinale, 21 – Roma;
- Ministero dell'Economia e delle Finanze in via Goito, 4 – Roma (solo consegna);
- altri enti e organizzazioni con sede all'interno del Grande Raccordo Anulare la cui attività è connessa con quella della Banca.

Le fattispecie in formato analogico gestite attraverso il SIR sono le seguenti:

- allegati in formato analogico a comunicazioni interne;
- fattispecie analogiche non documentali*;*
- documenti da trasmettere al CASC per il successivo invio tramite servizio postale;
- fattispecie cartacee non documentali e documenti in arrivo dall'esterno non gestiti attraverso il SGDD;
- documenti in arrivo dall'esterno gestiti attraverso il SGDD;
- documenti ricevuti direttamente dalle SO da trasmettere al CPAC per la protocollazione.

È vietato l'utilizzo del SIR nei confronti di destinatari e per il recapito di fattispecie diversi da quelli indicati.

5.5.2. Modalità di svolgimento del SIR

Il SIR viene effettuato tutti i giorni lavorativi, dal lunedì al venerdì (tranne il giorno in cui si svolge l'Assemblea Ordinaria dei Partecipanti al capitale della Banca) attraverso "giri di staffetta", secondo le modalità e negli orari comunicati dal Servizio GIN. Nelle giornate semifestive (14 agosto, 24 dicembre e 31 dicembre), il SIR è effettuato solo la mattina.

Le fattispecie da movimentare devono essere inserite in una bolgetta sigillata. La documentazione che, per la sua voluminosità, non può essere contenuta nella bolgetta deve essere chiusa in idonei contenitori sigillati, recanti l'indicazione del mittente. All'interno della bolgetta o del contenitore la documentazione deve essere a sua volta chiusa in buste recanti l'indicazione del mittente e del destinatario e differenziate attraverso l'uso di colori diversi in base al tipo di spedizione.

La consegna e il ritiro delle bolgette e dei contenitori viene effettuata, per quanto riguarda le SO ubicate a Palazzo Koch, di norma presso le unità segretariali; per le SO e gli enti ubicati in altri stabili, presso le portinerie o appositi armadi chiusi a chiave.

Nel caso di consegna presso le portinerie, le unità segretariali presenti nello stabile dovranno con cadenza quotidiana verificare la presenza di plichi destinati alle rispettive unità e ritirarli celermente. In caso non ci siano unità segretariali presso lo stabile, gli adempimenti di verifica e ritiro dei plichi saranno svolti dai Titolari o Sostituiti delle Unità di base o dai loro delegati.

In presenza di plichi erroneamente recapitati, sarà cura di chi li riceve restituirli immediatamente alla Divisione GEDOC.

Le bolgette e i contenitori ritirati vengono, di norma, consegnati alla Divisione GEDOC, dove sono aperti per lo smistamento dei plichi, il confezionamento delle bolgette e dei contenitori in partenza e il loro recapito in occasione del successivo giro di staffetta.

Gli enti e le organizzazioni di cui al 5.5.1 che non rientrano nei giri di staffetta provvedono direttamente alla consegna e al ritiro dei plichi di propria competenza presso la Divisione GEDOC.

Le operazioni di consegna e ritiro vengono effettuate senza il rilascio di ricevuta, ferma restando la facoltà delle SO e degli enti mittenti di richiederla direttamente alle SO o agli enti destinatari. Queste ricevute vengono restituite al mittente tramite il SIR, come pure le distinte di accompagnamento, firmate per ricevuta.

I mittenti devono valutare l'opportunità di veicolare, sotto la propria responsabilità, documenti di natura riservata attraverso il SIR.

Le bolgette vuote devono essere restituite immediatamente alla Divisione GEDOC tramite il SIR.

APPENDICE

I. ATTIVITÀ DEI CENTRI PROTOCOLLO (AC E FILIALI)

Gli atti notificati alla Banca d'Italia possono pervenire:

- in formato cartaceo, con consegna a mano dall'Ufficiale Giudiziario o altro messo notificatore allo sportello di ricezione della corrispondenza o tramite Poste Italiane con la consegna a domicilio (raccomandate);

- in formato elettronico, sulle caselle PEC di Filiale, sulla casella generalista PEC bancaditalia@pec.bancaditalia.it e sulla casella PEC comunicata al Ministero della Giustizia e pubblicata sul ReGIndE (DM 44/2011).

In fase di protocollazione di un atto notificato, l'addetto al CP dovrà compilare, nel *wizard* di protocollazione la scheda delle informazioni preliminari, scegliendo dal menu a tendina del campo "tipo documento" la "Tipologia Atto". I valori possibili sono:

a) "Atto giudiziario di competenza CSL"
b) "Procedura esecutiva contro dip./pens. BI", di competenza del Servizio Gestione del personale (GEP)
c) "Procedura esecutiva contro ADER", "Procedura esecutiva contro PA" e "Procedura esecutiva contro privati", di competenza del Servizio Tesoreria (TES)
d) "Atti tributari", di competenza del Servizio ACF
e) "Altri atti giudiziari": altri atti giudiziari notificati non rientranti tra quelli precedenti.

Per le categorie a), b), c), d) è prevista la valorizzazione automatica del campo "Assegnato a" non appena avvenuta la categorizzazione.

Atti giudiziari (lett. a)

Gli atti giudiziari che riguardano il contenzioso nei confronti della Banca relativi a procedimenti penali e civili di cognizione, anche sommaria, amministrativi e contabili sono di competenza della Consulenza Legale.

Questi atti contengono, normalmente nell'intestazione, l'indicazione delle seguenti autorità giurisdizionali:

- Tribunale amministrativo regionale (o T.A.R.)

- Consiglio di Stato (o C.d.S.)

- Corte dei conti

- Corte Costituzionale

- Corte di Cassazione

- Corte d'Appello

- Corte di Giustizia

- Tribunale di primo grado (o Tribunale dell'Unione europea)
- Corte europea dei diritti dell'uomo (o CEDU)
- Tribunale sezione(n) penale(n)
- Procura della Repubblica
- Giudice per le indagini preliminari (o GIP)
- Giudice dell'udienza preliminare (o GUP)
- Giudice di Pace

Oltre al nome dell'autorità giurisdizionale, gli atti contengono, nell'intestazione o nel corpo dell'atto, una o più delle seguenti espressioni:

- citazione (o cita)
- ricorso (o ricorre)
- reclamo (o reclama)
- opposizione
- appello
- revocazione
- revisione
- istanza o richiesta
- avviso
- udienza
- sentenza
- ordinanza
- decreto
- decreto ingiuntivo
- ingiunzione
- procedimento
- imputato

Le parole chiave indicate possono essere presenti anche all'interno delle relate di notifica o degli atti di comunicazione (comunicazione di cancelleria).

Gli atti giudiziari sono notificati a istanza di avvocati o di privati o tramite comunicazione (ad opera degli uffici giudiziari). Indipendentemente dalla tipologia (ricorso, appello, impugnazione, avviso, sentenza, ecc.), gli atti devono essere immediatamente assoggettati alla protocollazione ordinaria e assegnati, per competenza, alla sola Consulenza Legale.

I documenti in formato cartaceo devono essere prontamente trasmessi in originale. Il ritiro del documento da parte di un incaricato della Consulenza Legale deve avvenire con firma "per ricevuta". Tenuto conto dei rischi patrimoniali e reputazionali che possono derivare dal mancato o non tempestivo inoltro degli atti, il CP contatta immediatamente la Consulenza Legale in tutti i casi dubbi.

Non devono essere assegnati alla Consulenza Legale gli atti provenienti dalle Commissioni Tributarie e tutti gli atti relativi a procedimenti esecutivi nei quali la Banca assume il ruolo di terzo pignorato oppure di parte debitrice quali:

- atti di precetto;
- atti di pignoramento;
- ordinanze di assegnazione di somme;
- decreti, ordinanze in qualsiasi modo comunicati (tramite biglietto di cancelleria) o notificati (a istanza o dalla parte interessata) relativi a procedure esecutive contrassegnate da un numero di ruolo, normalmente indicato come NRE o RE (Numero Ruolo Esecuzioni o Ruolo Esecuzioni), RGE (Ruolo Generale Esecuzioni), RGEM (Ruolo Generale Esecuzioni Mobiliari) o EM (Esecuzioni Mobiliari), o recanti l'indicazione PPT (Pignoramento Presso Terzi) o simili.

Non devono inoltre essere assegnati alla Consulenza Legale, ancorché provenienti da uffici giudiziari:

- richieste di informazioni scritte alla P.A. ex art. 213 c.p.c.;
- ordini di pagamento emessi in controversie nelle quali la Banca non è parte, come ad esempio l'ordine di pagare una quota di stipendio al coniuge divorziato.

Non sono atti giudiziari e non vanno, neppure per conoscenza, assegnati alla Consulenza Legale i seguenti documenti:

- atti di accesso;
- diffide e atti di messa in mora;
- esposti, denunce e simili.

Atti tributari (lett. d)

Gli atti giudiziari, indipendentemente dalla tipologia (ricorso, appello, impugnazione, avviso, sentenza, ecc.), sono da assegnare al Servizio Assistenza e consulenza fiscale (ACF) se provengono da autorità della giurisdizione tributaria o contengono nell'intestazione:

- Commissione Tributaria Provinciale (o CTP)
- Commissione Tributaria Regionale (o CTR)

- Commissione Tributaria Centrale

Atti riguardanti procedimenti esecutivi (anche esattoriali ex art. 72 bis D.P.R. 602/73, lett. b), c)

Gli atti che riguardano procedimenti esecutivi in cui la Banca è coinvolta quale terzo pignorato devono essere assegnati in base alle indicazioni previste dalla Circolare n. 310 (*Testo unico delle disposizioni in materia di atti impeditivi)* e n. 317 (*Testo unico su retribuzioni e pensioni*). I procedimenti esecutivi contro soggetti privati (che non siano dipendenti o pensionati dell'Istituto) sono di competenza del Servizio Tesoreria dello Stato (TES).

Il trattamento documentale dei procedimenti esecutivi segue le regole della procedura ordinaria.

Fanno eccezione gli atti esecutivi contro dipendenti o pensionati dell'Istituto, che sono di competenza del Servizio Gestione del Personale (GEP)[54]. Essi debbono essere protocollati con l'attribuzione di riservato e trasmessi in originale a GEP previa scansione del documento. La scansione "per pronta informativa" deve essere menzionata nelle Annotazioni.

Nella procedura sono previste le seguenti categorie per gli atti esecutivi:

- Procedura esecutiva contro privati: procedimenti esecutivi contro banche e Poste italiane (tutti i Tribunali) e contro privati (diversi da dipendenti e pensionati della Banca), di competenza di TES - Divisione Atti impeditivi contro privati;

- Procedura esecutiva contro PA: procedimenti esecutivi contro Pubbliche Amministrazioni, di competenza di TES - Divisione Atti impeditivi di Tesoreria;

- Procedura esecutiva contro AdER: procedimenti esecutivi contro l'Agenzia delle Entrate-Riscossione (AdER), di competenza del Settore AdER costituito nell'ambito della Divisione Atti impeditivi contro privati del Servizio TES;

- Procedura esecutiva contro dip. / pens. BI: procedimenti esecutivi contro dipendenti o pensionati dell'Istituto, di competenza di GEP.

Altri atti giudiziari (lett. e)

La lettera e) comprende tutti gli atti non rientranti nelle categorie precedenti (ad es. multe, avvisi di liquidazione delle imposte, ecc.). All'atto della protocollazione l'addetto al CP deve valorizzare manualmente il campo con la Struttura assegnataria.

[54] Gli addetti al CPAC accedono ai dati anagrafici dei dipendenti/pensionati della Banca tramite una *query* in ambiente SAP.

II. PROCEDURA PER L'UTILIZZO DEL PROTOCOLLO DI EMERGENZA

Il DPR 445/2000 fissa i criteri e le modalità per la gestione elettronica dei documenti e nel Capo IV *Il sistema di gestione informatica dei documenti* prevede i casi in cui è necessario svolgere le operazioni di registrazione utilizzando un registro di protocollo di emergenza.

Autorizzazione all'utilizzo del protocollo di emergenza

Il Capo del Servizio Gestione dell'informazione (GIN), in qualità di responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 63 DPR 445/2000), è competente ad autorizzare la registrazione di protocollo, anche manuale, su uno o più registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura (cfr. anche Circolare n. 301). Qualora l'indisponibilità si prolunghi oltre ventiquattro ore, l'uso del Registro di protocollo di emergenza può essere autorizzato per un periodo massimo di sette giorni; il Registro deve comunque chiudersi il 31 dicembre di ogni anno. Il provvedimento di autorizzazione è soggetto a protocollo.

La Direzione della Struttura interessata può chiedere l'autorizzazione a utilizzare il protocollo di emergenza scrivendo alla casella GIN.ProtocolloEmergenza, mettendo in conoscenza la propria unità segreteriale. Il Servizio GIN trasmette l'autorizzazione via mail, indicando gli estremi del provvedimento di autorizzazione nonché i presidi di sicurezza da rispettare e incarica il Servizio Sviluppo informatico di fornire al Titolare della Struttura richiedente e della competente unità segretariale le password da utilizzare per l'accesso diretto alle proprie caselle PEC per la visualizzazione e protocollazione delle comunicazioni in ingresso.

Il Registro di protocollo di emergenza

Il Registro di protocollo di emergenza viene redatto e gestito in modalità decentrata:

- in Amministrazione centrale:
  - dal Centro Protocollo dell'AC, per la documentazione cartacea ricevuta dall'esterno e per quella digitale ricevuta sulla casella bancaditalia@pec.bancaditalia.it e sulla casella dedicata alla ricezione di atti giudiziari;
  - dalle Segreterie di Dipartimento, per la documentazione ricevuta dall'esterno della Banca e per quella prodotta presso ciascuna Struttura organizzativa del Dipartimento cui sia assegnato un indirizzo di posta elettronica ordinaria o certificata associato al sistema di gestione documentale digitale[55];
- nelle Filiali:
  - dal locale Centro di Protocollo per la documentazione in entrata e in uscita della Filiale stessa.

Nel Registro di protocollo di emergenza, da compilare su supporto digitale o, in caso di indisponibilità dei sistemi informatici, in formato cartaceo, devono essere riportate in premessa:

- causa tecnica dell'interruzione;
- data e ora di inizio dell'interruzione;
- estremi del provvedimento di autorizzazione del Servizio GIN;
- data e ora del ripristino della funzionalità del sistema, comunicata dal Servizio GIN.

Il Registro deve essere redatto utilizzando lo schema di seguito riportato:

[55] Il Punto di Ricezione (PDR) di via del Mille, 52, Roma, il Centro di protocollo del Servizio Segreteria particolare del Direttorio e comunicazione e il Centro di protocollo dell'Unità di informazione finanziaria, per i documenti di propria competenza, richiedono alle proprie Segreterie i numeri di protocollo in arrivo da utilizzare per protocollare i documenti cartacei ricevuti.

numero di protocollo	data di protocollo	Entrata /Uscita	mittente/ destinatario	oggetto	formato documento (Elettronico/Cartaceo)

Il numero di protocollo è formato da una sequenza numerica a 6 cifre progressiva preceduta dal codice della Struttura e seguita dall'anno di protocollazione indicato su due cifre. Ad esempio, per la documentazione del Servizio GIN la sequenza del numero di protocollo parte da 987-000001-aa[56]. La sequenza numerica utilizzata deve garantire l'identificazione univoca dei documenti registrati.

Per ogni giornata di utilizzo del Registro deve essere riportato il numero totale di operazioni effettuate manualmente.

I documenti in entrata devono essere inviati alla Struttura competente per la lavorazione subito dopo la registrazione di protocollo, possibilmente via mail (previa digitalizzazione di quelli cartacei, su cui deve essere apposto manualmente il numero di protocollo di emergenza). Gli originali cartacei devono essere conservati dal ricevente. Gli originali elettronici dei messaggi in arrivo vanno mantenuti nella stessa casella PEC di Struttura in cui sono stati reperiti: nessun messaggio deve essere spostato o cancellato dalla casella.

I documenti in uscita devono essere redatti preferibilmente in formato digitale (se possibile in formato pdf), indicando il numero di protocollo di emergenza, e firmati digitalmente, ove possibile, tramite l'utilizzo del *tool* di firma disponibile sulle postazioni di lavoro. L'invio delle comunicazioni può avvenire tramite le rispettive Segreterie, in modalità elettronica tramite gli indirizzi PEC di Struttura ovvero in modalità cartacea. Deve essere conservata una copia degli originali cartacei e dei *file* firmati digitalmente.

Conclusione dello stato di emergenza

Terminato lo stato di emergenza, l'autorizzazione all'utilizzo del protocollo di emergenza è revocata con provvedimento del Capo del Servizio GIN.

Una volta ritornati al normale funzionamento del sistema di protocollazione informatico, i dati relativi alle protocollazioni effettuate in emergenza devono essere immediatamente inseriti nel SGDD dalle unità che hanno utilizzato il Registro di protocollo di emergenza. A ciascun documento registrato in emergenza verrà attribuito nel SGDD un numero di protocollo secondo le modalità di seguito indicate. I documenti recheranno, pertanto, due numerazioni: quella del protocollo di emergenza e quella del protocollo generale.

Per i documenti cartacei ricevuti, ciascun Centro di Protocollo provvede alla digitalizzazione e protocollazione, secondo le modalità ordinarie indicate dal Manuale di gestione documentale; i documenti elettronici ricevuti sulle PEC gestite dal SGDD vengono protocollati automaticamente al momento della ripresa del funzionamento del sistema.

Tutti i documenti inviati (cartacei ed elettronici) devono essere inseriti e protocollati nel SGDD a cura delle Segreterie delle Strutture mittenti.

In tutti i casi, l'unità che ha gestito il protocollo di emergenza procederà ad associare alla scheda documentale, in un metadato dedicato, il numero e la data del protocollo di emergenza.

Le Segreterie che hanno aperto il Registro di emergenza (anche nel caso non abbiano protocollato nessun documento) devono trasmetterne copia all'indirizzo GIN.GestioneDocumenti@bancaditalia.it.

Il Servizio GIN è responsabile della raccolta e conservazione dei Registri di protocollo di emergenza ricevuti indicando:

[56] Per il Centro di protocollo dell'Amministrazione Centrale, deve essere utilizzato il codice CPAC.

- causa tecnica dell'interruzione;
- data e ora di inizio dell'interruzione;
- data e ora del ripristino della funzionalità del sistema;
- estremi del provvedimento di autorizzazione e di revoca;
- numero totale di operazioni registrate manualmente in ogni giornata.

Il Registro di protocollo di emergenza e una sua copia sono conservati in luoghi sicuri differenti.

III. ANNULLAMENTO DELLA PROTOCOLLAZIONE DELLE INFORMAZIONI OGGETTO DI REGISTRAZIONE DI PROTOCOLLO

La protocollazione dei documenti (sia nel caso di originali cartacei sia di originali digitali) può essere annullata nei seguenti casi:

- documenti erroneamente indirizzati alla Banca;
- documenti evidentemente stravaganti, palesemente privi di fondamento o che integrano l'ipotesi di *spamming*;
- documenti destinati alla Banca rientranti nelle fattispecie non gestite dal SGDD[57].

L'annullamento della protocollazione viene richiesto attraverso le funzioni del SGDD dal Titolare dell'UO assegnataria e approvato dall'UG; può essere effettuata solo dagli utenti con profilo CUO o livello superiore.

La fase di convalida dell'annullamento è accentrata presso gli utenti con ruolo UG, appartenenti a GIN. La conferma di annullamento da parte di GIN è puramente formale e non entra nel merito delle richieste pervenute.

É possibile ripristinare un documento di cui sia stato richiesto l'annullamento per errore contattando GIN tramite mail, da casella funzionale, all'indirizzo GIN.ERMES@bancaditalia.it.

Si ricorda che l'annullamento di un protocollo di un documento in partenza tramite PEC non ne interrompe il flusso in uscita. La spedizione via PEC, infatti, avviene istantaneamente al momento della protocollazione.

Le stesse modalità possono essere seguite per l'annullamento delle fatture passive e delle autofatture.

[57] Non rientrano in tale casistica le ricevute di consegna delle comunicazioni inviate via PEC, che devono essere invece conservate e recare i medesimi estremi di classificazione e fascicolazione del documento a cui si riferiscono.

IV. GESTIONE TELEGRAMMI

Ricezione e valore giuridico dei telegrammi in arrivo

I telegrammi vengono fatti recapitare senza indugio alla competente UO a cura degli addetti preposti alla loro ricezione.

Il telegramma ha l'efficacia probatoria della scrittura privata se l'originale consegnato all'ufficio di partenza è sottoscritto dal mittente, ovvero se è stato consegnato o fatto consegnare dal mittente, anche senza sottoscriverlo (art. 2705 c.c.).

Modalità di gestione documentale dei telegrammi in arrivo

I telegrammi non sono, di norma, gestiti attraverso il SGDD in quanto il sistema di trasmissione soddisfa di per sé il requisito della certezza documentale. Essi vanno conservati nel relativo fascicolo o sottofascicolo archivistico. Ove l'UO competente lo ritenga assolutamente necessario, i telegrammi possono essere trasmessi al competente CP per l'assoggettamento al trattamento previsto dal SGDD. La trasmissione deve essere, di norma, effettuata il giorno stesso della ricezione e, in ogni caso, con la massima tempestività al fine di consentire, ove possibile, la protocollazione nello stesso giorno. Qualora la data di protocollo sia successiva a quella di arrivo del telegramma, tale circostanza deve essere annotata nel registro di protocollo.

I telegrammi aventi contenuto di rilevanza temporanea sono conservati in ordine cronologico a cura dell'UO competente per almeno sei mesi e, quindi, distrutti informalmente a cura dell'UO medesima.

Spedizione e valore giuridico dei telegrammi in partenza

I telegrammi vengono predisposti e fatti spedire dalla competente UO secondo le modalità di legge, che ne assicurano carattere di ufficialità (art. 2705 c.c.), e non sono gestiti attraverso il SGDD.

I telegrammi aventi contenuto di rilevanza temporanea sono conservati in ordine cronologico a cura dell'UO competente per almeno sei mesi e, quindi, distrutti informalmente.

Nel caso in cui, a discrezione dell'UO, sia necessario mantenere traccia del telegramma, lo stesso deve essere conservato nel relativo fascicolo o sottofascicolo archivistico, ancorché non protocollato.

BANCA D'ITALIA
EUROSISTEMA

II. PARTE

BANCA D'ITALIA
EUROSISTEMA

MANUALE DI CONSERVAZIONE DOCUMENTALE

SOMMARIO

ELENCO DEGLI ACRONIMI

AC	Amministrazione Centrale
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
AS	Area Segretariale
ASBI	Archivio Storico della Banca d'Italia
CAD	Codice dell'Amministrazione Digitale
CASC	Centro di Assistenza Sociale e Culturale
CRI	Croce Rossa Italiana
D.lgs.	Decreto legislativo
DP	Dipartimento
DPR	Decreto del Presidente della Repubblica
GIN	Servizio Gestione dell'Informazione
ID	Codice identificativo
IPA	Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi
MIC	Ministero della Cultura
SCDI	Sistema di conservazione dei documenti informatici
SGDD	Sistema di gestione documentale digitale
SLT	Senza limiti di tempo – riferito alla conservazione
SO	Struttura Organizzativa
UO	Unità Operativa

1. INTRODUZIONE

1.1. AMBITO DI APPLICAZIONE E DEFINIZIONI

Il *Manuale di conservazione documentale* descrive le fasi di conservazione e scarto dei documenti, successive alle fasi di produzione, acquisizione e utilizzo descritte nel *Manuale di gestione documentale*.

In questo *Manuale* si definisce "documento" una rappresentazione di atti, fatti o dati giuridicamente rilevanti[1]. Sono definiti "documenti informatici" (o digitali) sia quelli direttamente prodotti in formato digitale sia le copie digitalizzate di documenti analogici[2].

Il complesso dei documenti prodotti o acquisiti dall'Istituto durante lo svolgimento della propria attività costituisce l'Archivio della Banca d'Italia, che rientra nella categoria dei beni culturali è destinato alla fruizione della collettività[3]; si articola in:

- Archivio corrente: l'insieme dei documenti necessari allo svolgimento delle attività in corso. Può contenere sia documentazione protocollata sia non protocollata, risalente a un termine di norma non superiore a tre anni per i documenti analogici, dopo il quale sono versati all'Archivio di deposito o scartati;
- Archivio di deposito: l'insieme dei documentati risalenti a un termine non superiore a quaranta anni. È organizzato in Archivio di deposito dell'Amministrazione Centrale (che comprende anche i documenti delle Delegazioni estere) e in Archivio di deposito delle Filiali. I documenti destinati alla conservazione senza limiti di tempo sono versati all'Archivio storico (ASBI), di norma dopo 25 anni dalla loro data di riversamento, per consentirne le lavorazioni propedeutiche alla successiva messa in consultazione; gli altri sono scartati;
- Archivio storico: l'insieme dei documenti prodotti, ricevuti o acquisiti dalla Banca da almeno quarant'anni, per i quali è prevista la conservazione senza limiti di tempo.

La conservazione è l'attività volta a proteggere e custodire nel tempo l'Archivio per preservare autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti, in modo che permanga il loro valore amministrativo e giuridico[4]. Nel caso di dati personali il processo di conservazione deve contemperare l'obbligo, previsto dal GDPR, di individuare un termine di conservazione dei dati personali propedeutico alla successiva eliminazione degli stessi, nel rispetto dell'obbligo, sancito dalla normativa sui beni culturali, di custodire e preservare le prerogative della documentazione di pubblico interesse per finalità storiche.

Quando il valore amministrativo e giuridico di un documento viene meno, il processo di selezione e scarto prevede, previa autorizzazione della competente Soprintendenza archivistica, la distruzione dei documenti secondo i criteri dettati dal *Piano di conservazione (Massimario di selezione e scarto)*, destinando all'Archivio storico quelli per i quali è prevista la conservazione senza limiti di tempo (SLT).

---

[1] Per maggiori informazioni cfr. *Codice dell'Amministrazione Digitale* (CAD), introdotto con il D.lgs. 82/2005.

[2] La Banca d'Italia utilizza tale tipo di documenti dal 22 giugno 2009 con l'introduzione del Sistema di gestione documentale digitale.

[3] Le principali disposizioni che disciplinano gli archivi degli enti pubblici sono: il D.lgs. 22 gennaio 2004, n. 42, *Codice dei beni culturali e del paesaggio*; il DPR 8 gennaio 2001, n. 37, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*; in base ai principi dettati dal Reg. Ue 2016/679 e dal D.lgs. 30 giugno 2003, n. 196 in tema di protezione dei dati personali, trovano applicazione le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica approvate dal garante* (Provv. n. 513 del 19 dicembre 2018).

[4] Per i documenti informatici il processo di conservazione è "a norma" se le relative procedure sono conformi alle *Linee guida dell'Agenzia per l'Italia Digitale* (AgID).

1.2. CONSERVAZIONE DEI DOCUMENTI

Nel sistema di conservazione operano tre soggetti con diversi ruoli e competenze:

- il "produttore" è l'addetto o i sistemi informativi che forniscono i documenti da conservare;
- il "responsabile" è il soggetto che definisce e attua le politiche di conservazione e ne governa la gestione. In Banca tale ruolo è svolto dal Capo del Servizio Gestione dell'informazione (GIN), che può delegare parte delle proprie funzioni ad addetti che abbiano maturato competenze ed esperienza nelle attività di gestione documentale;
- l'"utente" è l'addetto o il sistema che interagisce con il sistema di conservazione per accedere alle informazioni di interesse.

Tutti i documenti prodotti e acquisiti dalla Banca devono essere conservati per norma di legge per un periodo di tempo che varia in base al tipo di documento. I tempi di conservazione sono indicati nel *Piano di conservazione*, definito dal Servizio GIN.

Anche per la conservazione la Banca si configura come un'unica Area Organizzativa Omogenea (AOO), così come descritta nel Manuale di gestione documentale.

2. LA CONSERVAZIONE DEI DOCUMENTI DIGITALI

I documenti informatici protocollati sono conservati nel Sistema di conservazione dei documenti informatici (SCDI) contenuto all'interno del Sistema di gestione documentale digitale (SGDD), avviato il 22 giugno 2009. Il processo di conservazione si articola nelle seguenti fasi:

1. memorizzazione dei documenti informatici corredati da estremi di protocollo[5], dati di classificazione, fascicolazione e validazione digitale degli estensori, in formato PDF/A su idonei supporti che garantiscano la non modificabilità dei dati;
2. verifica del corretto svolgimento del processo di memorizzazione;
3. autenticazione per lotti dei dati da parte del Responsabile del SCDI o di un suo delegato, mediante apposizione della firma digitale;
4. attribuzione automatica del riferimento temporale che attesta il momento in cui il processo si è concluso.

I documenti informatici sono conservati in ordine cronologico e identificati per numero di protocollo. Alla fine del riversamento, il SCDI produce il Registro di protocollo (cfr. par. 2.2 del *Manuale di gestione documentale*). I dati e le informazioni vengono memorizzati su supporti informatici realizzati in due copie autentiche, conservate in luoghi diversi.

I documenti analogici dai quali è stata tratta la copia digitalizzata sono conservati dalla Struttura che ne ha curato la digitalizzazione, in ordine cronologico e mantenendo separati i documenti riservati e riservatissimi.

La consultazione dei documenti è consentita al solo Responsabile del SCDI e alle persone delegate. I documenti possono essere resi disponibili[6] mediante copia cartacea autenticata o in formato elettronico non modificabile a soggetti esterni alla Banca che abbiano per legge diritto all'accesso[7], previa richiesta inviata alla casella funzionale GIN.Archivio@bancaditalia.it .

I documenti informatici conservati attraverso il SCDI sono validi e rilevanti a tutti gli effetti di legge[8].

[5] I documenti in predisposizione e gli allegati non ufficiali (documentazione di supporto) dei documenti protocollati non sono conservati nel SCDI.

[6] Quando l'accesso (o l'esercizio di altro diritto di terzi) riguardi documenti contenenti dati personali, si applica quanto previsto dal Regolamento (Ue) 679/2016 e dal D.Lgs. 101/2018, recepiti dalla normativa interna sul trattamento dei dati personali (Circolare n. 257, cap. V).

[7] FOIA, Legge 241/1990, decreto legislativo n. 97/2016.

[8] Informazioni dettagliate sul processo di conservazione dei documenti digitali sono disponibili nella Parte III di questa Circolare, *Manuale tecnico di conservazione dei documenti digitali*, che descrive l'aderenza del processo di conservazione dell'Istituto alle regole tecniche in materia di sistema conservazione prescritte dalla normativa.

3. LA CONSERVAZIONE DEI DOCUMENTI ANALOGICI

I documenti analogici vengono custoditi in Archivio ordinati per unità archivistica[9].

Per i documenti protocollati dal 1° giugno 1989 al 21 giugno 2009, gli estremi di protocollo e le altre informazioni oggetto di registrazione sono reperibili nei relativi archivi elettronici.

3.1. ARCHIVIO CORRENTE

L'Archivio corrente dei documenti analogici si compone esclusivamente di documenti non protocollati, in quanto quelli protocollati sono tutti conservati nel SCDI (vedi par. 2).

La documentazione analogica non protocollata è conservata per tipologia di modulo o fattispecie, in ordine cronologico e per anno solare, per il tempo previsto nel Piano di conservazione. I documenti che rientrano nelle categorie da conservare SLT e gli originali cartacei provenienti dal Centro di Protocollo appartenenti alle categorie menzionate al par. 3.2.3 Parte I devono essere conservati separatamente dalla restante documentazione in attesa del riversamento all'Archivio di Deposito.

I documenti sono conservati in armadi chiusi a chiave; quelli riservatissimi devono essere custoditi in armadi di sicurezza.

I Titolari delle SO sono responsabili della corretta tenuta degli archivi correnti analogici contenenti documenti di pertinenza della Direzione, nonché in generale della tenuta degli archivi correnti delle UO facenti parte della struttura.

3.2. ARCHIVIO DI DEPOSITO DELL'AMMINISTRAZIONE CENTRALE

L'Archivio di deposito dell'AC, gestito dal Servizio GIN, è costituito dalla documentazione analogica, protocollata e non protocollata, proveniente dagli archivi correnti delle SO dell'AC ed elencata nel Repertorio d'archivio.

I documenti sono trasferiti dagli archivi correnti all'Archivio di deposito trascorso, di norma, un periodo di tre anni. Per esigenze operative, possono essere concordate tra le SO e il Servizio GIN modalità e tempistiche differenti per il trasferimento dei documenti sia dagli archivi correnti a quello di deposito che dagli archivi correnti direttamente all'ASBI.

I documenti sono trasferiti in Archivio di deposito ordinati in contenitori predisposti dalle UO trasferenti, recanti l'indicazione del contenuto e idonei a consentire l'agevole reperimento e la collocazione nelle scaffalature. I documenti riservati o riservatissimi sono trasferiti in contenitori sigillati. Per i documenti protocollati deve essere fornito anche l'elenco dei documenti presenti in ciascun contenitore; l'Archivio di deposito prende in carico i documenti verificando la corrispondenza degli elenchi.

I documenti non protocollati sono trasferiti su iniziativa delle UO compilando il modulo tipizzato "12 arch" presente nel SGDD, in cui, per le fattispecie non censite nel *Piano di conservazione,* dovrà anche essere proposto il tempo di conservazione. Il Servizio GIN provvede a determinare il termine di conservazione tenendo conto anche di quanto previsto per tipologie documentali simili. L'Archivio di deposito prende in carico i documenti riscontrando il numero dei contenitori, le tipologie e gli estremi cronologici, senza verificarne il contenuto, e ne dà ricevuta attraverso un'annotazione sul modulo.

L'eventuale riallocazione in contenitori diversi da quelli di origine viene effettuata mantenendo le indicazioni originarie e alla presenza di un delegato della struttura proprietaria della documentazione.

[9] Si intende per "unità archivistica" un insieme organico di documenti, raggruppati dal soggetto produttore per le esigenze della sua attività corrente o nel corso dell'ordinamento dell'archivio. È consentita la collocazione in un medesimo contenitore anche di più unità archivistiche di contenuto omogeneo.

I documenti riservati sono custoditi nei contenitori sigillati originari in locali o armadi chiusi a chiave; quelli riservatissimi devono essere custoditi in armadi di sicurezza.

Le chiavi sono detenute dal Capo del Servizio GIN o da un suo delegato.

3.3. ARCHIVI DI DEPOSITO DELLE FILIALI

Gli Archivi di deposito delle Filiali, gestiti dalle rispettive unità segretariali e sotto la responsabilità del Titolare della Filiale, sono costituiti dalla documentazione proveniente dagli archivi correnti delle relative UO. La documentazione custodita è elencata, a cura dell'unità segretariale, nel Repertorio d'archivio, da redigere in conformità allo schema disponibile nella intranet del Servizio GIN.

Il Repertorio d'archivio deve essere acquisito agli atti della Filiale come allegato a un documento interno recante la sottoscrizione del Titolare dell'unità segretariale e deve essere aggiornato in caso di trasferimenti dagli archivi correnti o operazioni di scarto.

I documenti sono trasferiti dall'Archivio corrente all'Archivio di deposito ordinati secondo le procedure descritte per l'AC. Il trasferimento viene attestato da documento interno a firma del Titolare dell'unità segretariale e dell'UO trasferente.

L'unità segretariale prende in carico i documenti riscontrando il numero di contenitori, le tipologie (fascicoli o fattispecie) e gli estremi cronologici, senza verifica del contenuto.

3.4. CONSULTAZIONE DEGLI ARCHIVI DI DEPOSITO

I documenti dell'Archivio di deposito dell'AC sono consultabili per esigenze di lavoro dagli addetti dell'UO trasferente o di quella eventualmente subentrata nelle competenze, previa richiesta inoltrata alla casella funzionale GIN.Archivio@bancaditalia.it. Nella richiesta devono essere indicati: le tipologie documentali da consultare, gli estremi cronologici, l'esigenza di consultazione, i nominativi degli addetti incaricati. Gli incaricati della consultazione possono fotocopiare i documenti o ritirare i documenti originali, trattenendoli per un periodo non superiore a tre mesi, previo rilascio di ricevuta. Copia della ricevuta è inserita nel contenitore in luogo di ogni documento ritirato.

Per le Filiali, la consultazione può avvenire previa richiesta scritta al Titolare della Filiale e successiva annotazione sulla scheda documentale degli estremi della richiesta, della data e del nominativo del consultante.

Nel caso di documenti riservati o riservatissimi, sia in AC sia nelle Filiali, la risigillatura dei relativi contenitori viene effettuata a cura degli incaricati della consultazione.

4. SELEZIONE E SCARTI D'ARCHIVIO

4.1. TEMPI DI CONSERVAZIONE

I tempi di conservazione, determinati tenendo presenti le esigenze attinenti alla conservazione dei documenti sia a fini amministrativi sia di ricerca storica, sono indicati nel *Piano di conservazione*.

A fattispecie documentali prodotte da più Strutture possono essere assegnati tempi di conservazione diversi, a seconda se le UO che li producono abbiano una specifica competenza in materia (cd. Strutture capofila) o meno. Le fattispecie delle UO capofila hanno tempi di conservazione più lunghi rispetto alla stessa fattispecie documentale prodotta da una struttura non capofila.

I tempi di conservazione decorrono:

- per la documentazione non protocollata, dal primo giorno dell'anno di riferimento di ricezione o creazione del documento;
- per la documentazione protocollata, dalla chiusura del fascicolo archivistico.

I documenti contenenti dati personali possono essere conservati e utilizzati anche oltre il periodo di tempo stabilito per il trattamento dei dati personali in essi contenuti, nel rispetto dei principi della normativa in materia e delle vigenti regole deontologiche e in quanto pertinenti e indispensabili per il perseguimento delle finalità di archiviazione nel pubblico interesse e di documentazione storica[10].

4.2. SELEZIONE E SCARTI D'ARCHIVIO IN AMMINISTRAZIONE CENTRALE

Il Servizio GIN individua i documenti che hanno raggiunto il termine del periodo di conservazione al fine di effettuarne lo scarto.

Sono sottoposte a procedura di scarto:

- le tipologie documentali che hanno maturato il periodo di conservazione fissato nel *Piano di conservazione*;
- le tipologie documentali eventualmente non censite nel *Piano di conservazione*, selezionate dal Servizio GIN sentite le SO competenti, ai fini della conferma del tempo di conservazione ritenuto congruo.

Il Servizio GIN compila un elenco in cui sono indicate le tipologie documentali da scartare con i relativi estremi cronologici e li trasmette alla Soprintendenza archivistica per il Lazio per l'autorizzazione allo scarto.

4.3. SELEZIONE E SCARTI D'ARCHIVIO NELLE FILIALI

La procedura di scarto viene attivata d'iniziativa da ciascuna Filiale con periodicità almeno quinquennale.

La Filiale compila gli elenchi di scarto, dove sono indicate le tipologie documentali da scartare con i relativi estremi cronologici. Gli elenchi di scarto relativi a tipologie documentali per le quali il *Piano di conservazione* prevede un tempo di conservazione di almeno trenta anni e quelle non censite sono trasmessi al Servizio GIN per il preventivo nulla-osta allo scarto.

Una volta ottenuti i nulla-osta, ciascuna Filiale trasmette gli elenchi alla competente Soprintendenza archivistica per l'autorizzazione allo scarto. Provvede poi alla cessione e alla distruzione dei documenti il cui scarto è stato autorizzato, secondo le modalità previste nel par. 4.5. Dell'avvenuto scarto deve essere fatta annotazione nel Repertorio d'archivio.

[10] Cfr. art. 99 e art. 101 del *Codice privacy*, D.lgs. 196/2003, Circ. 257/2004 (*Disposizioni in materia di trattamento dei dati personali*)

4.4. SELEZIONE E SCARTI D'ARCHIVIO NELLE DELEGAZIONI

La procedura di selezione e di scarto viene attivata periodicamente d'iniziativa da ciascuna Delegazione, che compila gli elenchi della documentazione selezionata, dove sono indicate le tipologie documentali e i relativi estremi cronologici, e li trasmette al Servizio GIN.

Ottenuta l'autorizzazione allo scarto, le Delegazioni effettuano la cessione e la distruzione in loco degli scarti d'archivio, nel rispetto delle normative nazionali del Paese ospitante.

Le Delegazioni devono cedere i documenti a conservazione SLT all'Archivio di deposito per il successivo trasferimento all'ASBI.

4.5. CESSIONE E DISTRUZIONE DEGLI SCARTI CARTACEI D'ARCHIVIO

I documenti riservati o riservatissimi da scartare sono sottoposti preventivamente a triturazione in loco mediante le apparecchiature in dotazione[11].

Per quanto riguarda i documenti non classificati, nel caso di quantità limitate da scartare, è facoltà delle Strutture scegliere di procedere comunque alla loro triturazione in loco.

Tutti i documenti (classificati e non) distrutti per mezzo dei trituratori in dotazione vengono trattati al pari del materiale a carattere non documentale (cfr. 4.6 Cessione del materiale a carattere non documentale).

I documenti che non siano stati preventivamente oggetto di distruzione devono essere immessi in sacchi sigillati, privi di involucri (contenitori o copertine di registri). La cessione di questi scarti deve avvenire in linea con la normativa esterna in materia di gestione dei rifiuti (cfr. Circolare 321/24, par. 3.4, Rifiuti da attività di scarto d'archivio).

La distruzione dei documenti negli impianti di destinazione avviene alla presenza di un incaricato della Banca[12]. Le operazioni vengono attestate da un verbale interno in cui devono essere indicati la tipologia e la quantità del materiale ceduto espressa in peso, a cui va allegata copia digitale della quarta copia del FIR. Il verbale deve essere sottoscritto dall'incaricato della Banca, vistato dal Titolare della SO e protocollato.

Le Filiali danno comunicazione al Servizio GIN dei metri lineari liberati in archivio, del peso del materiale distrutto e di eventuali ricavi ottenuti dalla cessione[13].

Le Filiali che effettuano lo scarto sono autorizzate alle spese necessarie per tali operazioni, tra cui trasporto, facchinaggio e missioni dei dipendenti.

4.6. CESSIONE DEL MATERIALE A CARATTERE NON DOCUMENTALE

Il materiale cartaceo a carattere non documentale, ivi compresa la carta da cestino, è ceduto quale atto di liberalità ai trasportatori autorizzati che svolgono il servizio di raccolta dei materiali cartacei per conto della CRI (a patto che essi provvedano al rilascio il FIR in occasione di ogni ritiro e assicurino l'effettuazione del servizio di ritiro in maniera efficiente) ovvero al gestore locale del servizio di raccolta dei rifiuti urbani.

---

[11] Cfr. Circolare n. 306, Cap. V, Par. 1, ove sono indicate le caratteristiche delle macchine da utilizzare.

[12] La presenza di un incaricato di Banca non è necessaria laddove l'impresa cui si conferiscono gli scarti d'archivio sia in grado di garantire la completa tracciabilità del processo di distruzione dei documenti.

[13] Gli eventuali importi ricavati da tale cessione sono versati a favore del bilancio dello Stato in conto entrate del Ministero dell'Economia e delle Finanza ("Entrate eventuali e diverse a favore del bilancio dello Stato"), i cui dati aggiornati andranno richiesti all'occorrenza al Servizio GIN.

4.7. SCARTO DEI DOCUMENTI ANALOGICI DIGITALIZZATI

I documenti originali analogici dei quali sia stata accertata la presenza nel SGDD di copia conforme digitale possono essere distrutti, purché il documento sia perfettamente leggibile. La verifica può essere effettuata a campione nella misura almeno del 10 per cento dei documenti compresi nel periodo soggetto allo scarto[14].

Nei casi in cui non sia possibile digitalizzare il documento originale[15] (ad es. perché troppo voluminoso oppure memorizzato su supporti diversi dal cartaceo), la copia fisica deve essere conservata nell'Archivio per il periodo temporale previsto dal *Piano di conservazione*.

Prima di procedere, le Filiali devono richiedere l'autorizzazione allo scarto alla Soprintendenza competente, indicando l'anno cui si riferiscono i documenti da distruggere. Per l'AC, la segnalazione è effettuata dal Servizio GIN.

Conclusi i controlli e ottenuta se del caso l'autorizzazione, entro il 30 settembre di ogni anno con riferimento ai documenti digitalizzati prima del biennio precedente[16]:

- le SO dell'AC inviano i documenti al Servizio GIN, che provvede materialmente alla distruzione;
- le Filiali distruggono i documenti in autonomia, dando notizia al Servizio GIN dell'avvenuto scarto e specificando metri lineari liberati in archivio e peso del materiale distrutto.

4.8. SCARTO DEI DOCUMENTI DIGITALI

Anche l'archivio digitale, al pari degli archivi cartacei, è sottoposto a interventi di scarto. Il Servizio GIN verifica periodicamente la documentazione scartabile in base al piano di conservazione e, una volta ottenuta l'autorizzazione dalla Soprintendenza del Lazio, avvia il processo di scarto, individuando i documenti in base al proprio codice identificativo univoco (ID univoco)[17].

I documenti digitali scartati sono censiti in un registro (Rapporto di scarto) che contiene gli ID univoci dei documenti sottoposti alla procedura e le informazioni utili a richiamare i *log* di sistema relativi all'intero processo. Il Rapporto di scarto costituisce una specifica tipologia documentale ed è anch'esso sottoposto al processo di conservazione.

Analogamente ai documenti analogici, anche per i documenti digitali a conservazione SLT è previsto il trasferimento della competenza all'ASBI.

[14] La percentuale del campione può essere aumentata in base al volume e alla rilevanza degli argomenti trattati. Nella scelta dei documenti da sottoporre a controllo, si può procedere con sorteggio casuale (ad esempio, documenti con protocollo pari o dispari) o su base numerica (ad esempio, un documento ogni 10). Nel caso in cui venissero riscontrate la mancanza del documento o la sua illeggibilità, si dovrà sanare la situazione e il controllo andrà esteso a tutti documenti del periodo.

[15] Si ricorda che alcuni Stati esteri non riconoscono il valore legale della firma digitale come paritetico a quello della firma chirografaria.

[16] In un'ottica prudenziale, le SO conserveranno la copia cartacea di tutti i documenti dell'ultimo biennio, procedendo di volta in volta alla distruzione di quelli antecedenti (quindi nel 2026 si possono scartare i documenti risalenti al 2023, nel 2027 quelli del 2024 e così via).

[17] L'ID univoco è un metadato associato al documento e consiste in un codice di 20 caratteri alfanumerici: i primi 6 identificano il soggetto produttore, gli altri 14 sono univoci per ogni documento. L'identificativo del soggetto produttore è il codice IPA (Indice delle Pubbliche Amministrazioni) della Banca.

BANCA D'ITALIA
EUROSISTEMA

III. PARTE

BANCA D'ITALIA
EUROSISTEMA

MANUALE TECNICO DI CONSERVAZIONE DEI DOCUMENTI DIGITALI

Adottato ai sensi degli artt. 20, commi 3 e 5-bis; 23-ter, c. 4; 43, commi 1 e 3; 44; 71 del D.Lgs. 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale*, delle *Linee guida* AgID sulla formazione, gestione e conservazione dei documenti informatici e dei seguenti articoli del DPCM 3 dicembre 2013 contenenti "Regole tecniche per il protocollo informatico":

- art. 2, c. 1 *Oggetto e ambito di applicazione*;
- art. 6 *Funzionalità*;
- art. 9 *Formato della segnatura di protocollo*;
- art. 18, commi 1 e 5 *Modalità di registrazione dei documenti informatici*;
- art. 20 *Segnatura di protocollo dei documenti trasmessi*;
- art. 21 *Informazioni da includere nella segnatura*.

SOMMARIO

ELENCO DEGLI ACRONIMI

AgID	Agenzia per l'Italia digitale
ASBI	Archivio Storico della Banca d'Italia
CD	*Compact disc*
D.Lgs	Decreto legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DVD	*Digital versatile disc*
FTP	*File transfer protocol*
GEDOC	Divisione Gestione dei documenti del Servizio Gestione dell'Informazione
ID	Identificativo univoco
IPdA	Indice Pacchetto di Archiviazione
IPA	Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi
ISO	*International standard organization*
OAIS	*Open archival information system*:
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
PdV	Pacchetto di versamento
PDF	*Portable document format*
PDI	Informazioni descrittive per la conservazione *(Preservation description information)*
RdV	Rapporto di versamento
SinCRO	Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali
SCDI	Sistema di conservazione dei documenti informatici
SGDD	Sistema di gestione documentale digitale
TSA	*Time Stamping Authority*
UNI	Ente nazionale italiano di unificazione
XML	*Extensible markup language*

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente *Manuale tecnico di conservazione dei documenti digitali* (di seguito, anche *Manuale*) illustra il modello organizzativo e il processo di conservazione dei documenti informatici prodotti o ricevuti, adottato dalla Banca d'Italia sia dal punto di vista organizzativo sia dal punto di vista tecnico ed operativo.

In particolare, il presente *Manuale*, a norma del paragrafo 4.6 delle *Linee Guida* AgID sulla formazione, gestione e conservazione dei documenti informatici, indica:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione e i tempi di scarto, così come indicati nel *Piano di conservazione*;
k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

La Banca d'Italia (di seguito, anche Banca) utilizza un Sistema di gestione documentale digitale (di seguito, anche SGDD) [1] per la tenuta del protocollo informatico, la gestione dei flussi documentali e la conservazione degli archivi ai sensi dell'art. 61 del DPR 28 dicembre 2000, n. 445 (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*, di seguito *Testo unico*).

I principi, le regole e le modalità di gestione dei documenti formati e acquisiti dalla Banca sono descritti e disciplinati nel *Manuale di gestione documentale*, pubblicato sul sito dell'Istituto (www.bancaditalia.it), cui si fa interamente riferimento.

Nell'ambito del SGDD, attraverso l'applicativo Virgilio prodotto da SIAV SpA, è realizzato il Sistema di conservazione dei documenti informatici (di seguito, anche SCDI), disciplinato dal presente *Manuale*.

[1] Il SGDD è operativo dal 22 giugno 2009.

2. NORMATIVA E STANDARD DI RIFERIMENTO

2.1. NORMATIVA DI RIFERIMENTO

Il presente *Manuale* è adottato ai sensi del paragrafo 4.3 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (nel seguito del documento "*Linee Guida AgID*"), nel rispetto della seguente normativa di riferimento:

- Codice Civile (Libro Quinto-Del lavoro, Titolo II-Del lavoro nell'impresa, Capo III-Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III-Disposizioni particolari per le imprese commerciali, Paragrafo 2-Delle scritture contabili, articolo 2215 bis - Documentazione informatica);
- Legge 7 agosto 1990, n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
- Decreto Legislativo 22 gennaio 2004, n. 42 - Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale (CAD), modificato e integrato con Decreto legislativo n. 179 del 26 agosto 2016;
- Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, aggiornato con Decreto Legislativo 10 agosto 2018 n. 101;
- Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Regolamento UE 910/2014 eIDAS (electronic IDentification Authentication and Signature), base normativa comune per i Paesi membri dell'UE per quanto riguarda i servizi fiduciari, i mezzi di identificazione elettronica e le modalità di interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni;
- Art. 25 (Anticipazione obbligo fattura elettronica) del DL 24 aprile 2014, n. 66 (Misure urgenti per la competitività e la giustizia sociale), convertito, con modificazioni, dalla Legge 23 giugno 2014, n. 89;
- Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, L. 24 dicembre 2007, n. 244;
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto- articolo 21, comma 5, del decreto legislativo n. 82/2005;
- Circolare Agenzia delle entrate n. 36 del 6 dicembre 2006 (Decreto ministeriale 23 gennaio 2004 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto);
- Circolare Agenzia delle entrate n. 18/E del 24 giugno 2014 - IVA – Ulteriori istruzioni in tema di fatturazione;
- Risoluzione n. 46/E Agenzia delle Entrate 10 aprile 2017 - Termini per la conservazione dei documenti rilevanti ai fini tributari;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 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 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 digitale, 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 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;
- Artt. 19-22 del Decreto Legge 22 giugno 2012, n. 83 - Misure urgenti per la crescita del Paese, convertito, con modificazioni, dalla Legge 7 agosto 2012, n. 134, con cui è stata istituita l'"Agenzia per l'Italia Digitale" (AgID);
- Deliberazione CNIPA 21 maggio 2009, n. 45 – Regole per il riconoscimento e la verifica del documento informatico;
- Misure minime di sicurezza ICT emanate dall'AgID con Circolare n. 2/2017;
- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (emanate da AgID con determinazioni n. 121 e 147 del 2019);
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (emanate da AgID con determinazioni n. 407/2020 e n. 371/2021 e s.m.i.);
- Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato il 25 giugno 2021 con determinazione AgID n. 455/2021. Tale Regolamento definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, fissando in un apposito allegato i requisiti generali nonché i requisiti di qualità, di sicurezza e organizzazione necessari per la fornitura del servizio. Composto di due allegati tecnici, il Regolamento è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del Decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020.

2.2. STANDARD DI RIFERIMENTO

Nel rispetto degli standard e delle specifiche tecniche di cui all'allegato 4 delle *Linee guida* l'attività di conservazione si basa sui seguenti standard:

- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- EAD (3)/ISAD (G);
- ETSI TS 101 533-1 V1.3.1 (2012-04) -*Technical Specification, Electronic Signatures and Infrastructures* (ESI); *Information Preservation Systems Security*; Part 1: *Requirements for Implementation and Management*, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) - *Technical Report, Electronic Signatures and Infrastructures* (ESI); *Information Preservation Systems Security*; Part 2: *Guidelines for Assessors*, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ISO 14721:2012 - OAIS *(Open Archivai Information System),* Sistema informativo aperto per l'archiviazione;
- ISO 15836:2009 - *Information and documentation - The Dublin Core metadata element set*, Sistema di metadati del Dublin Core;
- ISO/IEC 27001:2013 - *Information technology - Security techniques - Information security management systems - Requirements,* Requisiti di un ISMS *(Information Security Management System*);
- SCONS2/EAG/ISDIAH;
- UNI 11386:2010 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

3. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE, RUOLI E RESPONSABILITÀ

ruoli	attività di competenza	struttura	soggetto	eventuali deleghe
Responsabile del servizio di conservazione	• gestione amministrativa del sistema di conservazione dei documenti informatici (SCDI) • autenticazione per lotti dei dati da parte del Responsabile del SCDI o di uno dei suoi delegati, mediante apposizione della propria firma digitale • scarto dei pacchetti di archiviazione, previa autorizzazione delle Autorità archivistiche, sulla base del Massimario di conservazione e di scarto Di concerto con il Servizio Sviluppo informatico: • governo della gestione del Sistema di Conservazione • verifica periodica di conformità a normativa e standard di riferimento. Di concerto con il Servizio Sviluppo Informatico: • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici	**Servizio Gestione dell'informazione**	**Capo Servizio**	Personale dell'Area Manageriale e Alte professionalità formalmente delegato dal Capo del Servizio Gestione dell'informazione
Responsabile della sicurezza dei sistemi per la conservazione	• rispetto e monitoraggio dei requisiti di sicurezza del Sistema di Conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	**Servizio Gestione Sistemi Informatici**	**Capo Servizio**	
Titolare del trattamento dei dati personali	• garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali	**Banca d'Italia nel suo complesso**	**Direttore generale**	Servizio Organizzazione

Responsabile dei sistemi informativi per la conservazione	• gestione tecnica del SCDI (applicazione informatica, piattaforma tecnologica e archivi di dati) • acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento • preparazione e gestione del pacchetto di archiviazione • su richiesta, preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche. Di concerto con il Servizio Gestione Sistemi Informatici: • monitoraggio del sistema di conservazione	**Servizio Sviluppo Informatico**	**Capo Servizio**	
Responsabile sviluppo e manutenzione del sistema di conservazione	• conduzione e manutenzione del sistema di conservazione • *change management*	**Servizio Sviluppo Informatico**	**Capo Servizio**	

4. OGGETTI SOTTOPOSTI A CONSERVAZIONE

4.1. CLASSI DOCUMENTALI OGGETTO DI CONSERVAZIONE

Sono sottoposti a conservazione tutti i documenti gestiti nel SGDD completi dei relativi metadati, appartenenti alle classi documentali di seguito specificate[2]:

- Esterni (ambito: Protocollo - in arrivo)
- Interni (ambito: Protocollo - in uscita e interni)
- Notifica in uscita (ambito: Registro Documenti fiscalmente rilevanti)
- Notifica in entrata (ambito: Registro Documenti fiscalmente rilevanti)
- Fattura nazionale (ambito: Registro Documenti fiscalmente rilevanti)
- Fattura estera (ambito: Registro documenti fiscalmente rilevanti)
- Autofattura - Intra (ambito: Registro documenti fiscalmente rilevanti)
- Fattura (ambito: Fatture attive)
- Notifica (ambito: Fatture attive)
- Esterni eProc (ambito: Protocollo *e-procurement* - in arrivo)
- Report protocolli giornalieri (ambito: Registro mensile /Registro giornaliero di protocollo)

Per ciascun oggetto sottoposto a conservazione, sono conservati il *file* digitale e i metadati.

Per quanto riguarda il *file* digitale, i documenti sono conservati nel formato descritto e disciplinato nel *Manuale di gestione documentale.*

Di seguito l'elenco dei formati accettati dal sistema di conservazione Virgilio.

Formato	Proprietario/Gestore del formato	Estensione	Tipo Mime	Aperto	Visualizzatore
PDF, PDF/A	Adobe Systems	.pdf	Application/pdf	Sì	Adobe Reader
TIFF	Aldus Corporation	.tif	Image/tiff	No	Visualizzatori di immagini
JPEG	Joint photographic experts group	.jpeg .jpg	Image/jpeg	Sì	Visualizzatori di immagini
Office, Open XML	Microsoft	.docx, .xlxs, .pptx	MIME	Sì	Visualizzatori compatibili
XML	W3C	.xml	Application/xml text/xml	Sì	Web browser
TXT	txt/plain	.txt	ASCII, UTF-8, UNICODE	Sì	Visualizzatori di testo
PEC, EMAIL	Vari	.eml	RCF 2822/MIME	No	Client di posta elettronica che supportano la visualizzazione di file .eml
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	Application/vnd.oasis opendocument.text	Sì	Visualizzatori di immagini

Nei paragrafi seguenti vengono specificati i metadati oggetto di conservazione digitale per ciascuna classe documentale.

[2] Gli allegati non ufficiali non vengono protocollati e pertanto non vanno in conservazione.

4.1.1. Esterni (Ambito: Protocollo - in arrivo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto Conservatore
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Mittente	SÌ	Mittente o destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	SÌ	Registro Ufficiale
Titolo	SÌ	Codice di classificazione
Classe	SÌ	Codice di classificazione
Sottoclasse	SÌ	Codice di classificazione
Data ricezione	NO	
Protocollo mittente	NO	
Data - Protocollo mittente	NO	
Formato	NO	Cartaceo/Elettronico
Procedimento amministrativo	NO	

4.1.2. Interni (Ambito: Protocollo - in Uscita e Interni)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Destinatario	SÌ	Destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Mittente	SÌ	Soggetto/ufficio titolare del procedimento - Struttura/Filiale
Impronta	SÌ	Impronta
Archivio		Registro Ufficiale
Titolo	SÌ (Classificazione)	Codice di classificazione
Classe	SÌ (Classificazione)	Codice di classificazione
Sottoclasse	SÌ (Classificazione)	Codice di classificazione
Protocollo mittente	NO	
Data protocollo mittente	NO	
Unità	NO	
Formato	NO	
Tipo di spedizione	NO	
Tipo comunicazione	NO	
Copie cartacee	NO	SÌ/NO
Procedimento amministrativo	NO	

4.1.3. Notifica in uscita (Ambito: Registro Documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto (Esito e descrizione - tipo ricevuta)	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Mittente (o Codice struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Unità (o Codice ufficio, se presente)	NO	
Impronta	SÌ	Impronta
Identificativo SDI	NO	
Formato	NO	
Stato	NO	
Fornitore	NO	
Partita IVA - Codice fiscale	NO	
Riferimento Fattura	NO	
Data Fattura	NO	
Nome *File*	NO	

4.1.4. Notifica in entrata (Ambito: Registro Documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto (esito e descrizione - tipo ricevuta)	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura (o Codice Struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Formato	NO	
Data Ricezione	NO	
Stato	NO	
Nome *file*	NO	
Identificativo SDI	NO	

4.1.5. Fattura nazionale (Ambito: Registro Documenti fiscalmente rilevanti)

Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura (o Codice Struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Data ricezione	NO	
Archivio	NO	
Fornitore	NO	
Partita Iva	NO	
Codice Fiscale	NO	
Riferimento fattura	NO	
Data fattura	NO	
Formato	NO	
Stato documento	NO	
Progressivo univoco	NO	

4.1.6. Fattura estera (Ambito: Registro documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	**Obbligatorietà**	**Riferimento normativa**
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Fornitore	SÌ	Mittente
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura (o Codice struttura, se presente)	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Partita Iva	NO	
Riferimento fattura	NO	
Data fattura	NO	
Formato	NO	
Stato documento	NO	

4.1.7. Autofattura - Intra (Ambito: Registro documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Fornitore	SÌ	Mittente
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura (o Codice ufficio, se presente)	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Partita Iva	NO	
Codice Fiscale	NO	
Riferimento fattura	NO	
Data fattura	NO	
Rif. n. protocollo	NO	
Rif. data protocollo	NO	
Stato documento	NO	

4.1.8. Fattura (Ambito: Fatture attive)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Soggetto/ufficio titolare del procedimento
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Destinatario	SÌ	Destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Impronta	SÌ	Impronta
Tipo spedizione	NO	
Denominazione	NO	
Data registrazione	NO	
Numero documento	NO	
Partita IVA	NO	
Codice Fiscale	NO	
Archivio	NO	
Tipologia documentale	NO	

4.1.9. Notifica (Ambito: Fatture attive)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	NO	
Tipologia documentale	NO	
Formato	NO	
Data ricezione	NO	
Stato	NO	

4.1.10. Esterni eProc (Ambito: Protocollo *e-procurement* - in arrivo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo *e- procurement*	SÌ	Numero di protocollo
Data Protocollo *e- procurement*	SÌ	Data di protocollo
Mittente	SÌ	Mittente o destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	SÌ	Registro Ufficiale
Titolo	SÌ	Codice di classificazione
Classe	SÌ	Codice di classificazione
Sottoclasse	SÌ	Codice di classificazione
Tipo esterno	NO	
Formato	NO	Cartaceo/Elettronico
Procedimento amministrativo	NO	

4.1.11. Report protocolli giornalieri (Ambito: Registro mensile/Registro giornaliero di protocollo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa[3]
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Numero progressivo del registro	SÌ	Numero di protocollo
Data di creazione del registro	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Codice identificativo del Registro	NO	Identificazione degli allegati
Responsabile gestione documentale	NO	Soggetto/ufficio titolare del procedimento
Classificazione	NO	Codice di classificazione
Impronta	SÌ	Impronta
Protocollo iniziale (numero prima registrazione)	SÌ	
Protocollo finale (numero ultima registrazione)	SÌ	
Data prima registrazione e data ultima registrazione	NO	

[3] Per il registro giornaliero di protocollo si fa riferimento al set di metadati fornito dall'AgID nel documento "Istruzioni per la produzione del registro giornaliero di protocollo".

4.2. FASCICOLI

Un documento viene immesso nel sistema di conservazione solo dopo il suo inserimento in un fascicolo. Per "fascicolo" si intende l'aggregazione documentale di cui all'all. 5 delle *Linee Guida AgID*. L'inserimento di ciascun documento oggetto di conservazione nel relativo fascicolo di appartenenza viene effettuata dal soggetto/ufficio titolare del procedimento, attraverso apposite funzioni nel SGDD.

In tabella sono riportati i metadati dell'aggregazione documentale "fascicolo".

Metadati inviati in conservazione digitale	**Obbligatorietà**	**Riferimento normativa**
IdAgg	SÌ	ID Aggregazione
Tipologia fascicolo	SÌ	Tipologia fascicolo
Soggetti	SÌ	Soggetti
Assegnazione	SÌ	Assegnazione
Data apertura	SÌ	Data apertura
Classificazione	SÌ	Classificazione
Progressivo	SÌ	Progressivo
Chiave descrittiva	SÌ	Chiave descrittiva - Oggetto
Data chiusura	NO	Data chiusura
Procedimento amministrativo	SÌ	Procedimento amministrativo
Indice documenti	SÌ	Indice documenti
Posizione fisica aggregazione documentale	Obbligatoria solo per i fascicoli ibridi	Posizione fisica aggregazione documentale
IdAggPrimario	NO	Identificativo dell'Aggregazione Primaria
Tempo di conservazione	SI	Tempo di conservazione
Note	NO	Note

Solo per la tipologia fascicolo "Procedimento amministrativo" sono inoltre presenti i seguenti ulteriori metadati:

Metadati inviati in conservazione digitale	**Obbligatorietà**	**Riferimento normativa**
Preparatoria – Data inizio fase	NO	Procedimento Amministrativo
Preparatoria – Data fine fase	NO	Procedimento Amministrativo
Istruttoria – Data inizio fase	NO	Procedimento Amministrativo
Istruttoria – Data fine fase	NO	Procedimento Amministrativo
Consultiva – Data inizio fase	NO	Procedimento Amministrativo
Consultiva – Data fine fase	NO	Procedimento Amministrativo
Decisoria o deliberativa – Data inizio fase	NO	Procedimento Amministrativo
Decisoria o deliberativa – Data fine fase	NO	Procedimento Amministrativo
Integrazione dell'efficacia – Data inizio fase	NO	Procedimento Amministrativo
Integrazione dell'efficacia – Data fine fase	NO	Procedimento Amministrativo

5. IL PROCESSO DI CONSERVAZIONE

5.1. ASPETTI GENERALI

Il processo di conservazione avviene con cadenza periodica secondo le regole tecniche stabilite dalla normativa ed è articolato nelle seguenti fasi:

- memorizzazione dei documenti informatici;
- verifica del corretto svolgimento del processo di memorizzazione;
- autenticazione per lotti dei dati da parte del Responsabile del SCDI[4] mediante firma digitale;
- attribuzione automatica del riferimento temporale che attesta la conclusione del processo.

I documenti informatici sono conservati in ordine cronologico e identificati per numero di protocollo. Alla fine del riversamento il SCDI produce il Registro di protocollo. I dati e le informazioni vengono memorizzati su supporti informatici realizzati in due copie autentiche, conservate in luoghi diversi[5].

L'accesso ai dati, in formato consultabile, è consentito al Responsabile del SCDI e alle persone da lui autorizzate. L'esibizione a soggetti esterni alla Banca che ne abbiano titolo di documenti presenti nel SCDI può essere effettuata mediante copia cartacea autenticata o in formato elettronico non modificabile, previa richiesta alla casella funzionale GIN.Archivio@bancaditalia.it.

5.2. MODELLO ORGANIZZATIVO INTERNO

Il modello organizzativo adottato dalla Banca per la conservazione digitale è coerente con lo standard internazionale OAIS per la conservazione di oggetti digitali a lungo termine[6].

Nel sistema di conservazione operano tre soggetti con diversi ruoli e competenze:

- il "produttore" è identificato negli addetti o nei sistemi informativi che forniscono i documenti da conservare;
- il "responsabile" è identificato nel Capo del Servizio GIN, che definisce e attua le politiche complessive del processo e del sistema e ne governa la gestione con piena responsabilità. Può delegare parte delle proprie funzioni ad addetti che abbiano maturato competenze ed esperienza nelle attività di gestione documentale;
- l'"utente" è identificato negli addetti o sistemi che interagiscono con il sistema di conservazione al fine di ricercare le informazioni di interesse.

L'Istituto, ai sensi dell'art. 44 del CAD e dell'art. 4.3 delle *Linee Guida AgID*, gestisce al proprio interno la conservazione dei documenti informatici dallo stesso prodotti e acquisiti attraverso il sistema di conservazione denominato Virgilio, fornito da Siav S.p.A.

Il mantenimento nel tempo del valore legale dei documenti e i processi di verifica/integrità dei supporti virtualizzati sono assicurati da una serie di servizi automatici di gestione e manutenzione dell'archivio digitale tra cui:

- gestione multi-azienda/multi-ente, che permette di suddividere l'archivio digitale per azienda o ente; per ciascuno di essi è possibile attribuire diversi profili e ruoli per l'accesso ai dati e l'esecuzione delle attività di conservazione;
- gestione per ambiti, che consente di organizzare logicamente l'archivio definendo ambiti documentali distinti (relativi, ad esempio, alle diverse tipologie documentali);
- gestione per classi o tipologie documentali, che permette di rintracciare un documento tramite una serie di dati allo stesso associati.

[4] Tutte le azioni di competenza del Responsabile possono essere compiute dal soggetto delegato.
[5] I documenti analogici dai quali è stata tratta la copia digitalizzata sono conservati dalla Struttura che ne ha curato la digitalizzazione e soggetti a scarto secondo quanto disposto al par. 4.7.
[6] Conformemente alla previsione di cui all'allegato 4 delle *Linee Guida AgID*.

Il sistema di conservazione Virgilio gestisce il *workflow* relativo a tutte le fasi del processo conservativo che vengono controllate e monitorate.

Il processo di conservazione descritto nel presente *Manuale* viene costantemente aggiornato (con contestuale aggiornamento del *Manuale* stesso) a seguito di interventi normativi, introduzione di nuove tipologie sottoposte a conservazione o modifiche al modello organizzativo e/o al processo di conservazione.

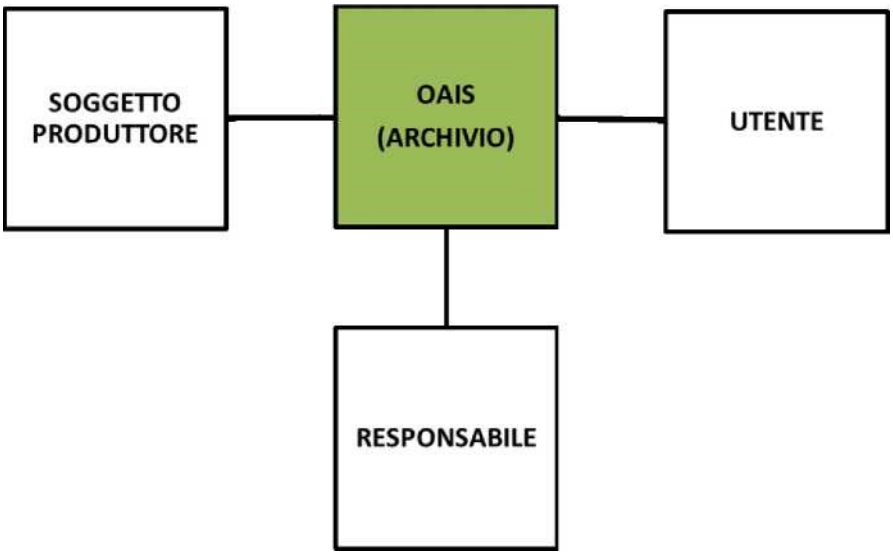

Figura 1 Virgilio - modello OAIS

5.3. IL PROCESSO DI CONSERVAZIONE

Gli oggetti digitali sottoposti al processo di conservazione sono organizzati in pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare (documenti informatici, aggregazioni informatiche), comprensivi delle informazioni per la loro interpretazione e rappresentazione. I pacchetti informativi contengono non solo il documento e/o l'aggregazione informatica ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo.

Secondo il modello OAIS, il SCDI adotta procedure in grado di garantire la conservazione nel lungo periodo monitorando tutte le attività inglobate nelle tre fasi principali di:

- immissione nel sistema di conservazione;
- certificazione e conservazione;
- distribuzione ed esibizione all'utenza.

La trasmissione delle informazioni tra il produttore e il Sistema di conservazione e tra questo e l'utente avviene attraverso pacchetti informativi che, a seconda della loro funzione, si distinguono in tre tipologie:

- Pacchetto di Versamento (PdV);
- Pacchetto di Archiviazione (PdA);
- Pacchetto di Distribuzione (PdD).

Nei successivi paragrafi sono illustrate le principali fasi del processo di gestione e conservazione (schematizzato nella Figura 2) dal momento della trasmissione del PdV da parte del soggetto produttore fino alla creazione del PdD.

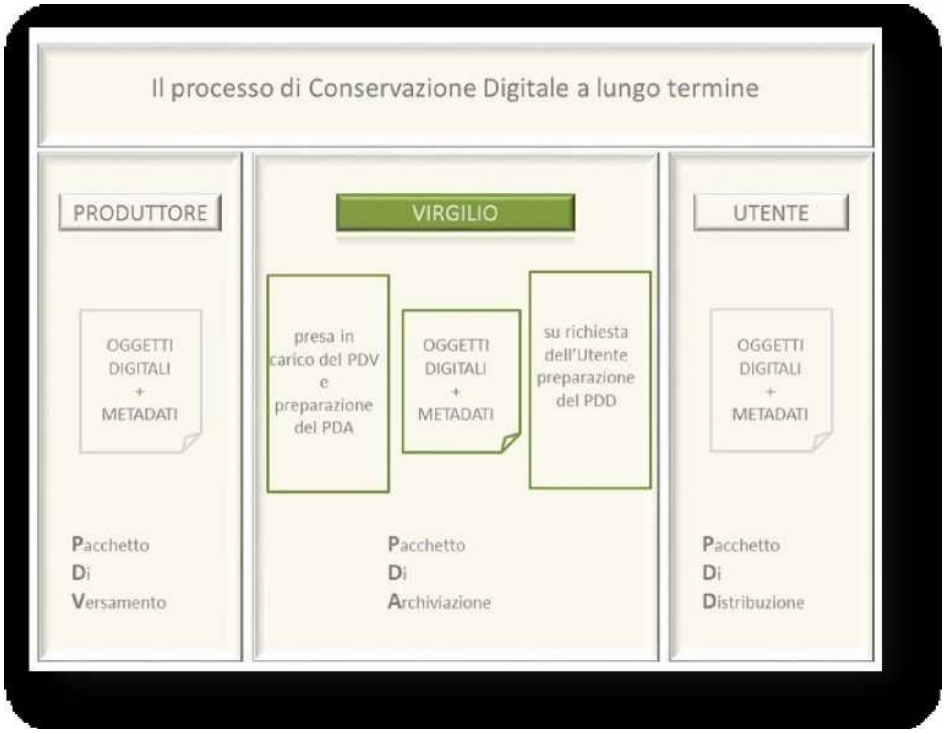

Figura 2 Schema del processo di conservazione

5.4. CREAZIONE DEL PACCHETTO DI VERSAMENTO (PDV)

Il PdV è l'insieme di oggetti digitali e metadati (risorse digitali) provenienti dal soggetto produttore e versati nel sistema di conservazione. Il processo di acquisizione individua le attività finalizzate all'accettazione delle risorse digitali versate dal soggetto produttore e alla loro preparazione per l'inserimento nell'archivio. Il Responsabile del servizio di conservazione è responsabile del coordinamento dell'intero processo e del monitoraggio delle attività.

Viene verificata in modo automatico la presenza dei metadati obbligatori e aggiuntivi associati alle tipologie/aggregazioni documentali informatiche da versare nel sistema e, se presenti, si procede alla lavorazione del PdV; altrimenti è effettuata una pre-lavorazione per attribuire i metadati al documento.

I metadati che devono essere presenti in un documento informatico sono:

- Identificativo
- Modalità di formazione
- Tipologia documentale
- Dati di registrazione
- Chiave descrittiva
- Soggetti
- Allegati
- Classificazione
- Riservato
- Identificativo del formato
- Verifica
- IdAgg
- Identificativo documento primario
- Nome del documento
- Versione del documento

- Tracciature modifiche documento
- Tempo di conservazione
- Note
- data di chiusura
- oggetto (sintesi del contenuto di un documento)
- soggetto produttore
- destinatario.

I metadati per il documento amministrativo informatico sono:

- codice identificativo dell'amministrazione (codice IPA);
- codice identificativo dell'area organizzativa omogenea (codice univoco IPA dell'AAOO);
- codice identificativo del registro;
- data di protocollo;
- progressivo di protocollo.

I documenti digitali vengono trasferiti sul *filesystem* di Virgilio tramite connettore "nativo" al SGDD. I documenti sono trasferiti nell'area dedicata di presa in carico; i *file* da elaborare vengono suddivisi per tipologia documentale e scaricati in cartelle appositamente predisposte. Viene verificata la presenza di ulteriori metadati inerenti il contesto e l'integrità degli oggetti/aggregazioni documentali versati nel sistema ovvero delle informazioni descrittive per la conservazione a lungo termine dei PdA.

A ogni documento versato in conservazione il sistema associa automaticamente una serie di metadati di processo; tra questi assume particolare importanza il codice alfanumerico identificativo univoco (d'ora in poi ID univoco[7]) del soggetto produttore assegnato ad ogni oggetto/aggregazione documentale informatica.

L'ID univoco ha una duplice funzione:

- segna la tracciabilità del documento durante l'intero processo di conservazione;
- identifica in modo univoco il soggetto produttore.

Il soggetto produttore, dopo aver trasferito il PdV nell'area di presa in carico, invia l'impronta (contenente l'*hash*) dei documenti inserendola tra i metadati. Al momento della presa in carico del PdV il sistema ricalcola automaticamente l'impronta di ogni documento e la confronta con quella indicata nei metadati. In questo modo viene garantita l'integrità dei documenti, in quanto si ha la sicurezza che non siano intervenute perdite di dati durante le fasi di lavorazione.

[7] L'ID univoco è un codice di 20 caratteri alfanumerici: i primi 6 caratteri identificano il soggetto produttore e sono comuni a tutti gli oggetti documentali versati nel sistema da parte del medesimo produttore; restanti 14 sono univoci per ogni documento versato nel sistema. L'identificativo del soggetto produttore coincide con il codice IPA della Banca.

5.5. FASE DI VERSAMENTO

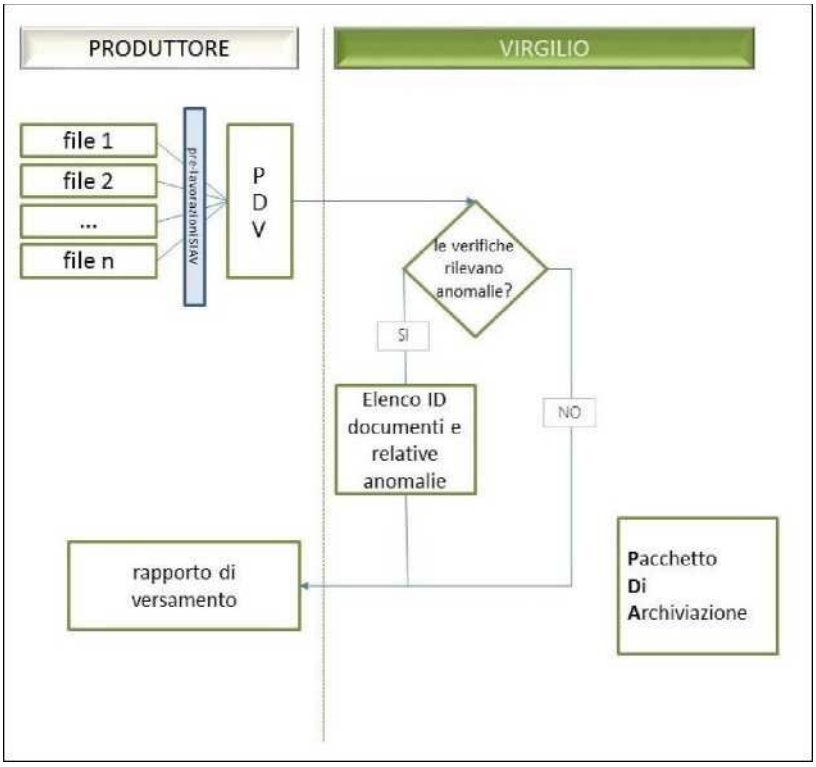

Figura 3 Fase di versamento

La Figura 3 illustra il flusso di lavoro dell'intera fase di versamento, dal trasferimento dei documenti/aggregazioni informatiche da parte del soggetto produttore fino alla formazione del PdA.

5.6. VERIFICHE, ECCEZIONI E RAPPORTO DI VERSAMENTO

L'acquisizione dei PdV nel sistema di conservazione avviene a cadenza programmata. Per ogni pacchetto ricevuto, Virgilio verifica automaticamente che il contenuto sia rispondente a quanto previsto e confronta l'impronta ricalcolata del documento con quella inviata dal soggetto produttore, per verificare l'integrità della documentazione trasmessa. Qualora vengano rilevate anomalie, il sistema provvede a notificarle al produttore.

Il Responsabile del servizio di conservazione dispone lo svolgimento di periodici controlli sui documenti e sulle aggregazioni documentali presenti nel sistema tramite i rapporti di versamento prodotti dal SCDI, in modo da identificare eventuali anomalie rispetto ai formati destinati alla conservazione. È comunque possibile modificare/integrare l'elenco dei formati ammessi, stabilendo eventuali eccezioni[8].

I controlli effettuati da Virgilio sui documenti e sulle aggregazioni informatiche versate dal soggetto produttore comprendono anche le verifiche volte a identificare il formato dei *file*[9].

[8] Le eccezioni fanno riferimento alla necessità, da parte del soggetto produttore, di conservare i documenti in formati non compatibili con la conservazione a lungo termine e sui quali non sia possibile effettuare una conversione di formato senza alterarne la leggibilità e la forma. In questo caso il Responsabile del servizio di conservazione ammette tali documenti nel sistema di conservazione, specificando che non è possibile assicurarne l'integrità e la leggibilità per la conservazione a lungo termine.

[9] Comunemente il formato di un *file* è riconosciuto attraverso la sua estensione; ai fini di una corretta identificazione questo non è però sufficiente, in quanto l'estensione di un *file* può essere modificata, volontariamente o involontariamente (ad esempio a causa di una ridenominazione accidentale o per l'intervento di un virus). In ogni caso, l'identificazione del *file* tramite l'estensione permette di riconoscere solo la famiglia di formati cui appartiene e non la specifica versione, utile ai fini di una corretta rappresentazione del *file*.

Per la verifica dei formati[10] all'interno di Virgilio si utilizzano dei *tool* di riconoscimento basati sull'identificazione di particolari sequenze composte in modo variabile da 2 a 10 *byte* che si trovano in specifiche posizioni del *file* (comunemente all'inizio).

Effettuata la verifica del formato, il sistema genera automaticamente il Rapporto di Versamento (RdV), che contiene un riferimento temporale. Il Rapporto è un *file* in formato .xml che attesta l'esito di versamento del PdV trasferito dal Titolare al SDC, che per ciascun *file* incluso nel PdV riporta le seguenti informazioni:

- URN, stringa univoca che identifica il documento;
- metadati del singolo *file*;
- impronta del *file*.

Il Sistema di conservazione genera in automatico il RdV che viene reso disponibile al Titolare; contestualmente alla generazione del RdV, viene segnalato anche l'esito del conferimento, che può essere positivo, nel caso in cui non siano state evidenziate anomalie, oppure negativo se il sistema identifica un errore o un'anomalia del PdV.

I rapporti di versamento vengono salvati dal sistema e versati in conservazione; Virgilio raggruppa la tipologia documentale "rapporto" che, per ogni soggetto produttore, include tutti i rapporti di versamento.

5.7. RIFIUTO DEL PACCHETTO DI VERSAMENTO

Nel caso in cui le verifiche diano esito negativo, il sistema segnala la presenza di un'anomalia[11] e rifiuta i documenti. Virgilio segnala i documenti anomali contenuti nel PdV all'interno del rapporto di versamento per il successivo intervento di risoluzione dell'anomalia, rielaborazione e reinvio del PdV.

5.8. PACCHETTO DI ARCHIVIAZIONE

Il pacchetto di archiviazione (PdA) è il pacchetto di informazioni destinato alla conservazione a lungo termine ed è un'aggregazione di quattro tipi di oggetti informativi:

- il contenuto informativo *(content information* - CI), che include i dati di interesse primario, ossia le informazioni destinate alla conservazione e le informazioni di rappresentazione associate, ad es. uno specifico documento XML e lo schema XML relativo;
- le informazioni descrittive per la conservazione (PDI), che includono le informazioni di identificazione dell'oggetto digitale, di contesto, provenienza e integrità;
- le informazioni sull'impacchettamento (*packaging information* - PI), cioè le informazioni sulla composizione del pacchetto informativo (al fine di collegare l'oggetto digitale e i metadati associati);
- le informazioni descrittive, finalizzate a sostenere l'accesso alle risorse/contenuto informativo mediante strumenti di ricerca o di recupero.

Il PdA si ottiene dalla trasformazione di uno o più PdV attraverso le operazioni di conservazione a lungo termine (*archival storage*) delle risorse digitali affidate a Virgilio.

La componente *archival storage* conserva i documenti garantendo l'integrità e la fruibilità a lungo termine delle sequenze di bit (*bit stream*) e ne permette il recupero per eventuali consultazioni.

Il Responsabile della conservazione della Banca dispone il periodico aggiornamento dei PdA per la migrazione dei formati. Inoltre, d'accordo con i responsabili della sicurezza e dei sistemi informativi della Banca, aggiorna le politiche di recupero in caso di incidente (*disaster recovery*).

[10] Per la lista dei formati accettati cfr. *Manuale di gestione documentale.*

[11] Si hanno documenti anomali in presenza di corruzione o perdita di dati (ad esempio i dati sono memorizzati su formati non compatibili, metadati mancanti, documenti con firma scaduta).

Il PdA (Figura 4) prevede una specifica strutturazione in formato XML secondo quanto definito dallo standard UNI SinCRO[12].

Le informazioni PDI costituiscono metadati fondamentali per la conservazione a lungo termine dei documenti; tali informazioni sono articolate in cinque aree:

- Provenienza: informazioni relative alla provenienza del contenuto informativo ovvero dati sulla natura giuridica, organigramma e funzionigramma del soggetto produttore e tracciabilità dei cambiamenti avvenuti;
- Identificazione: informazioni che identificano in maniera univoca gli oggetti digitali (ad es. data e numero di protocollo);
- Integrità: informazioni sulla verifica della firma e impronta dell'autore del documento/aggregazione informatica;
- Contesto: informazioni che mostrano le relazioni esistenti tra il contenuto informativo e il contesto in cui è stato prodotto (es. l'ID del documento, il Piano di classificazione);
- Diritti: informazioni sui diritti di accesso al contenuto informativo.

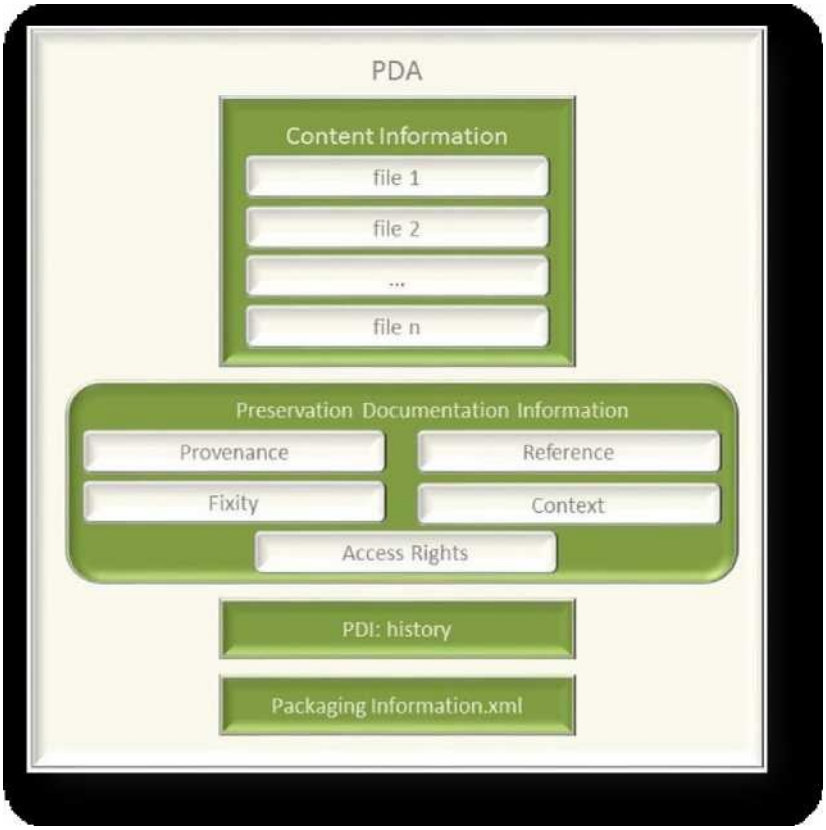

Figura 4 Schema del PdA

5.9. CREAZIONE E STRUTTURA

Il sistema di conservazione gestisce esclusivamente PdA omogenei, che sono formati accorpando documenti informatici della stessa tipologia.

[12] Tale standard definisce, nel rispetto del modello OAIS, una struttura di dati XML che consente di predisporre sia le informazioni identificative minime (previste dal legislatore) sia un'infrastruttura generale in grado di gestire tutte le informazioni archivistiche necessarie al processo di formazione e tenuta dei documenti informatici in modo da assicurare l'interoperabilità tra sistemi e la conservazione a lungo termine.

Virgilio scompatta i PdV suddividendo i documenti in base alla tipologia documentale cui appartengono; per ogni tipologia documentale viene formato un PdA (Figura 5).

Se nel PdV sono presenti documenti fiscali su cui vanno effettuati i controlli di continuità (ad esempio fatture), il sistema procede ad accorpare i documenti appartenenti alla stessa tipologia documentale e a ordinarli, effettuando successivamente i controlli sulla numerazione dei documenti. Se vengono riscontrate anomalie, il sistema provvede automaticamente a bloccare la formazione del PdA, a segnalare il problema e a richiedere un nuovo invio. Il sistema sospende il processo per quello specifico PdA fino all'invio del documento rettificato. Dopo il nuovo invio vengono effettuati di nuovo i controlli di continuità e, in caso di esito positivo, il sistema procede alla formazione del PdA.

Una volta formato, il PdA viene firmato digitalmente dal Responsabile del servizio di conservazione.

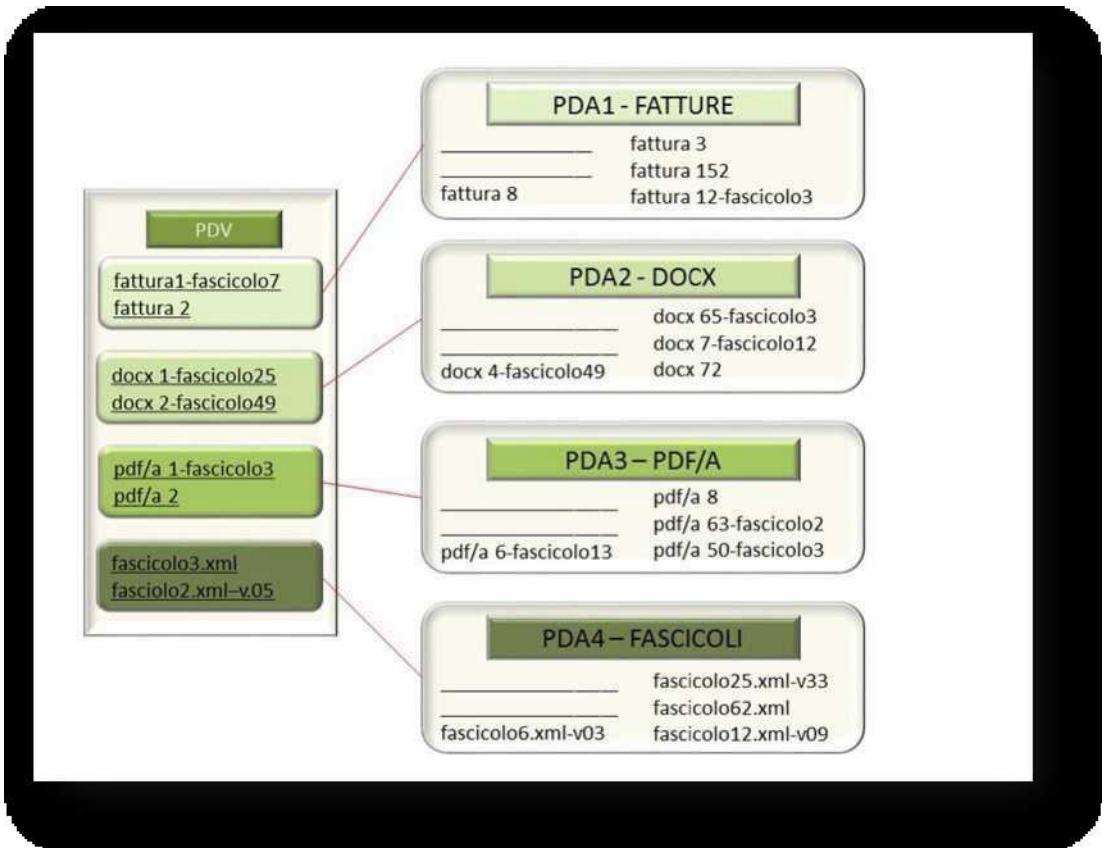

Figura 5 Formazione del PdA

5.10. L'INDICE DEL PACCHETTO DI ARCHIVIAZIONE

Il lotto di documenti sottoposti a conservazione viene riepilogato in un *file* di chiusura, detto Indice del Pacchetto di archiviazione (IPdA), il quale costituisce l'evidenza informatica associata ad ogni PdA.

Attraverso l'IPdA si può procedere alla verifica delle informazioni archivistiche necessarie al processo di tenuta dei documenti/aggregazioni informatiche e obbligatorie per assicurare le garanzie di affidabilità, integrità e autenticità nel lungo periodo.

Le informazioni archivistiche obbligatorie racchiuse in un IPdA sono:

- descrizione generale, che comprende l'identificativo univoco dell'IPdA e le informazioni relative all'applicazione che lo ha generato (nome e versione dell'applicativo e produttore del *software*). Nel caso di modifica del contenuto di un PdA già presente all'interno del sistema di

conservazione, si includeranno nell'IPdA i riferimenti relativi ad esso;

- attributi del relativo PdA, che comprendono l'identificativo univoco del PdA e, eventualmente, i riferimenti che permettono di collegare tale PdA ad altri PdA presenti all'interno del sistema di conservazione come descritto al punto precedente;
- *file* gruppo, che permette di aggregare più oggetti documentali presenti all'interno del PdA indicandone l'identificativo univoco e l'impronta. Tale attributo consente di formare degli insiemi di oggetti sulla base di criteri funzionali;
- processo, attraverso il quale vengono inserite le informazioni riguardanti il processo di conservazione dello specifico PdA cui l'IPdA fa riferimento. Sono riportati i dati dei soggetti intervenuti durante il processo di formazione del PdA, le informazioni relative a data e ora di produzione dell'IPdA sotto forma di riferimento temporale; è previsto un campo *Extrainfo* in cui il sistema riporta le informazioni utili a richiamare i *log* di sistema salvati e conservati nel *database* Oracle.

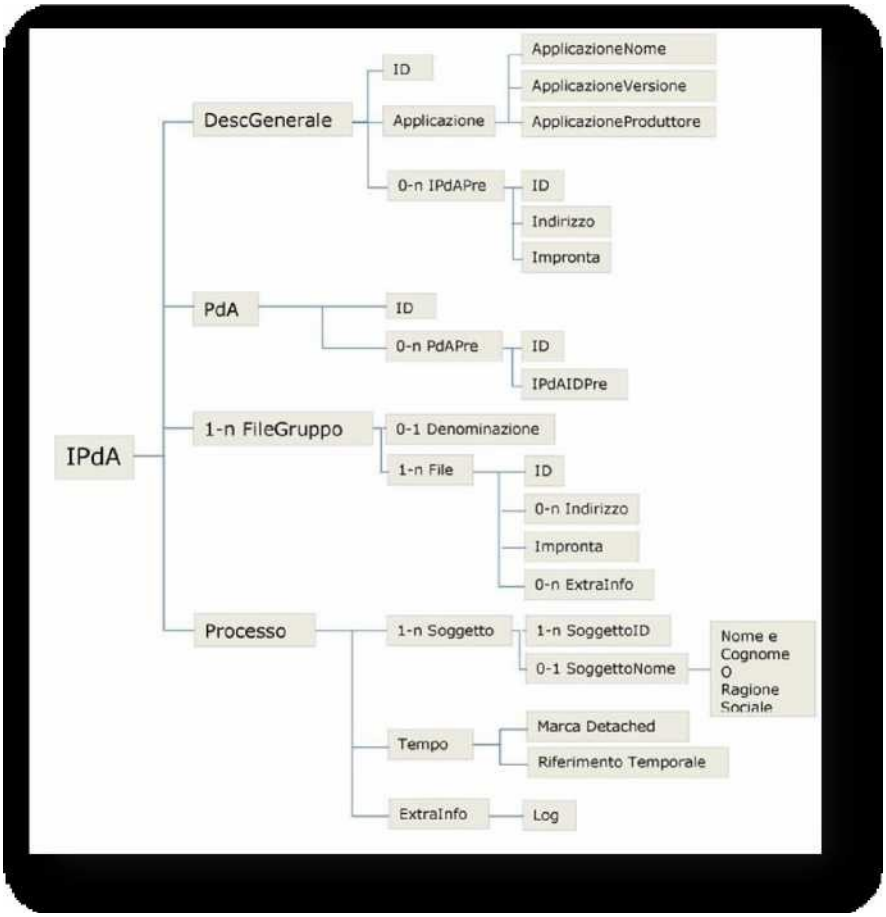

Figura 6 Struttura dell'IPdA

5.11. RICHIESTA DI ESIBIZIONE E DIRITTI D'ACCESSO

Il documento conservato deve essere leggibile in qualunque momento e disponibile su richiesta anche su supporto ottico e/o analogico. La richiesta di esibizione deve essere inoltrata al Servizio GIN.

I soggetti produttori possono essere autorizzati ad accedere direttamente, tramite *username* e *password* forniti dal conservatore, alla *console web* di esibizione di Virgilio e a ricercare i documenti di interesse.

5.12. CREAZIONE ED ESIBIZIONE DEL PACCHETTO DI DISTRIBUZIONE

In base agli ID univoci forniti dal soggetto produttore al momento della richiesta, il sistema localizza i documenti conservati nei diversi PdA ed effettua un duplicato. I duplicati sono inseriti all'interno di un unico PdD, che viene firmato digitalmente dal Responsabile del servizio di conservazione e salvato

nel formato di *file* immagine ISO; a questo punto il sistema produce il PdD. Virgilio restituisce un messaggio di avvenuta presa in carico, in cui viene indicato il *link* del canale FTP o FTPS dal quale si può procedere a scaricare il *file* immagine ISO del PdD.

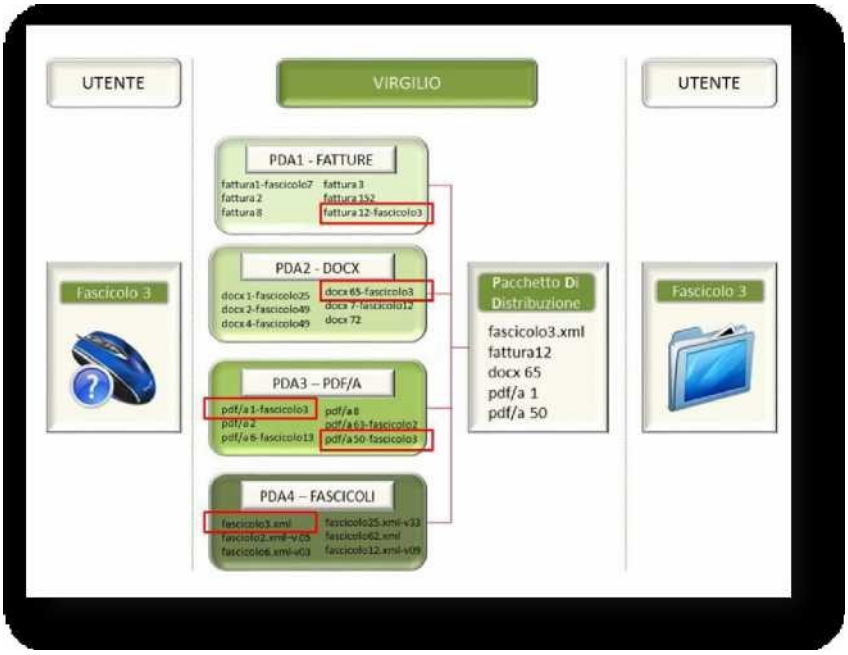

Figura 7 Schema del processo di esibizione

5.13. STRUTTURA DATI PER GLI OGGETTI DIGITALI E PER I METADATI

Le informazioni necessarie alla conservazione degli oggetti digitali, e relativi metadati, vengono organizzate in *file* XML conforme allo standard UNI SInCRO e salvate all'interno della base dati del SdC.

Per ogni tipologia di oggetti digitali sottoposti alla conservazione viene definito uno specifico set di metadati suddiviso, al suo interno, in due subset: metadati obbligatori[13] e facoltativi.

La memorizzazione dei metadati collegati al documento digitale avviene all'interno di un *file* XML conservato all'interno della base dati del SdC. Parallelamente il documento digitale a cui fanno riferimento i metadati e la sua impronta sono conservati in un *repository* dedicato all'interno della base dati del SCDI[14] e indicizzato per successive interrogazioni.

Nel caso del PdD il salvataggio avviene su *file system* e non all'interno della base dati. Il reperimento dell'oggetto digitale avviene in maniera trasparente se si utilizza il visualizzatore proprio del SCDI; in alternativa è sempre possibile risalire al documento attraverso i suoi metadati per il tramite dell'IPdA[15] UNI SInCRO.

[13] Con le *Linee Guida* entrate in vigore nel 2022 non si parla più di metadati minimi.
[14] Il salvataggio è organizzato secondo una struttura di cartelle organizzata in base a soggetto produttore, data e ora del versamento.
[15] Gli oggetti digitali sono raggiungibili consultando direttamente l'IPdA e il *file*, specificato nella sezione "*documentspath*" inserita in "mediainfo". L'accesso agli oggetti digitali avviene utilizzando come chiave di accesso l'indice del documento, specificato per ogni *file*, e la posizione nel *repository* del PdD, che viene estratta dal *file* indicato in "*documentspath*".

6. IL PROCESSO DI SELEZIONE E SCARTO DEI DOCUMENTI DIGITALI

Il processo di selezione e scarto include gli interventi finalizzati:

- alla conservazione senza limiti di tempo (SLT) della documentazione di interesse storico;
- allo scarto della restante documentazione dopo che questa ha maturato i tempi di conservazione previsti dal *Massimario di selezione e di scarto*[20], previa autorizzazione della Soprintendenza archivistica del Lazio.

Per i documenti a conservazione SLT è previsto il trasferimento della competenza all'ASBI.

Il Responsabile del sistema di conservazione verifica periodicamente la documentazione scartabile in base al piano di conservazione e, una volta ottenuta l'autorizzazione dalla Soprintendenza del Lazio, avvia il processo di scarto localizzando i documenti in base al proprio codice identificativo univoco (ID univoco).

I documenti digitali scartati sono censiti in un registro (Rapporto di scarto) che contiene gli ID univoci dei documenti sottoposti alla procedura e le informazioni utili a richiamare i *log* di sistema relativi all'intero processo[16]. Il Rapporto di scarto costituisce una specifica tipologia documentale e pertanto è anch'esso sottoposto al processo di conservazione.

Nel caso in cui il processo di scarto coinvolga tutti i documenti contenuti in un unico PdA, il sistema provvede a cancellare fisicamente l'intero PdA dall'archivio. In questo caso nel rapporto di scarto viene riportato anche l'ID del PdA oltre a quello dei documenti ivi contenuti.

[16] Virgilio applica un filtro che impedisce la visualizzazione e la modifica dei documenti scartati.

7. SICUREZZA LOGICA E FISICA DEI DOCUMENTI CONSERVATI

7.1. CONTROLLI SULLA LEGGIBILITÀ

Conservare un contenuto informativo digitale significa mantenere nel tempo la capacità di riprodurlo con il contenuto e la forma originaria. In altre parole, significa mantenere, attraverso il sistema di conservazione, la capacità di leggere la relativa sequenza binaria nella sua interezza, interpretarla con le regole del formato elettronico e visualizzare il documento risultante a video, a stampa o su un altro dispositivo di output.

Per mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità di tutti i documenti conservati nel sistema, è stato predisposto un piano della sicurezza volto ad individuare e correggere tempestivamente eventuali processi di corruzione dei documenti e dei supporti.

Il Responsabile del servizio di conservazione pianifica la tempistica e le attività per la verifica dei documenti conservati. Alcune verifiche vengono effettuate automaticamente dal sistema, che seleziona un campione casuale di documenti dall'intero archivio di ogni soggetto produttore, calcola l'impronta di ogni documento e la confronta con quella rilevata al momento dell'acquisizione del documento stesso da parte del sistema di conservazione e che si trova memorizzata tra i metadati[17].

La leggibilità dei documenti conservati è assicurata attraverso:

- il confronto dell'impronta, in quanto la corruzione della stringa di *bit* che compone il documento provocherebbe la visualizzazione a schermo in maniera distorta[18];
- la possibilità di reperire strumenti *software* e *hardware* in grado di visualizzare il documento.

Il Responsabile del servizio di conservazione garantisce l'aggiornamento dei formati e dei supporti utilizzati all'interno del sistema di conservazione e, nel caso individui un caso di obsolescenza tecnologica[19], attua tempestivamente il piano di riversamento.

7.2. PRODUZIONE DI COPIE E DUPLICATI

Il salvataggio dei dati avviene con frequenza almeno settimanale. Inoltre sono gestite periodicamente le procedure per la produzione di copie e duplicati dei PdA e PdD. Le copie informatiche dei documenti contenuti in un PdA sono identiche ai documenti originali[20].

La copia conforme al documento informatico originale viene prodotta su richiesta del soggetto produttore. Nel caso in cui un documento debba essere esibito in giudizio o in altra sede ufficiale, il Responsabile della conservazione attesta la conformità della copia prodotta all'originale.

Due copie di sicurezza dei PdA vengono prodotte nel momento in cui il PdA viene generato, sono memorizzate automaticamente sui *server* e conservate in luoghi diversi.

È possibile, in situazioni particolari, generare copie anche su supporti fisici (CD, DVD, *pendrive*); ogni copia ISO è corredata di un numero progressivo del PdA e dalla tipologia di documenti che contiene. Le etichette poste sul singolo supporto devono contenere:

- identificativo/nome/ragione sociale del soggetto produttore;

[17] Se l'impronta risulta valida, significa che la stringa di *bit* che forma il documento informatico è rimasta invariata e non sono occorse nel tempo delle corruzioni, volontarie o involontarie, che possano aver cambiato la forma e/o il contenuto del documento. Attraverso il confronto delle impronte è possibile verificare, oltre all'integrità, anche l'autenticità del documento. Infatti, la modifica o la rimozione delle firme digitali e delle marche/riferimenti temporali apposte al documento andrebbe a modificare la stringa di *byte* che lo compone, causando la generazione di un'impronta differente.

[18] Il grado di perdita di leggibilità dipende dal livello di corruzione intervenuto e dalla solidità del formato in cui il documento è salvato.

[19] L'obsolescenza tecnologica fa riferimento agli effetti del progresso tecnologico e dell'introduzione sul mercato di tecnologie sempre più avanzate, che causa il disuso di formati e supporti precedenti.

[20] Il duplicato informatico è il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della stessa sequenza di valori binari del documento originario.

- data di masterizzazione e numero della copia;
- informazioni sul PdA conservato (oggetti e tipologia dei documenti archiviati nel supporto);
- la data di prima certificazione della copia ISO che contiene;
- gli estremi cronologici di ogni copia ISO ivi contenuta.

7.3. VERIFICHE, RIVERSAMENTO E MONITORAGGIO

L'integrità, la leggibilità dei dati e la robustezza dei supporti sono soggette a verifica periodica; in caso di obsolescenza, si procede alla generazione di copie e al riversamento[21].

Nel corso di un periodo di conservazione dei documenti, può essere necessario trasferire il contenuto da un supporto di memorizzazione a un altro. Tale esigenza può presentarsi, ad esempio, nel caso in cui sia necessario creare copie di *backup* o in caso di obsolescenza tecnologica dei supporti.

L'operazione deve essere effettuata dal Responsabile del servizio di conservazione e assume il nome tecnico di "processo di riversamento diretto". Il riversamento diretto prevede che le informazioni riportate sul nuovo supporto non subiscano alcuna modifica[22].

Periodicamente viene garantita la conformità degli archivi digitali conservati attraverso i seguenti interventi:

- controlli di processo, per lo più automatizzati dal sistema, sulle fasi operative del processo di conservazione e sulla gestione delle anomalie;
- controlli periodici pianificati preventivamente dai responsabili della conservazione e dei sistemi informativi;
- controlli e manutenzione delle strutture *hardware* e *software*.

Il Servizio Gestione sistemi informatici, quale responsabile dei sistemi e della sicurezza informatica, effettua e monitora le procedure di *backup*; d'intesa con il Responsabile del servizio di conservazione, coordina anche le attività previste per il piano di gestione di continuità operativa e del *risk assessment* indicate nel Piano per la sicurezza.

Il sistema effettua diversi controlli:

- tracciamento e monitoraggio di tutte le attività del processo di conservazione e di gestione dei supporti, notificando gli esiti delle diverse attività svolte, così come eventuali problemi, anomalie e criticità;
- verifica, per ogni documento conservato, di leggibilità, integrità, valore legale e livello di obsolescenza del formato;
- rinnovo automatico del periodo di validità dei certificati dei documenti, tracciando e segnalando gli esiti.

Tutti gli esiti delle operazioni svolte, incluse le anomalie e le situazioni critiche o potenzialmente rischiose evidenziate dal sistema di conservazione, sono visualizzabili sui *report* disponibili *online* attraverso la *console* di gestione.

[21] Il riversamento è il processo attraverso il quale si riproducono i documenti affidati a dispositivi di memorizzazione digitali. Le tipologie di riversamento sono due: diretto e sostitutivo; si differenziano per il tipo di risultato che producono.
[22] Per certificare che questo accada, il sistema calcola automaticamente un'impronta dei documenti registrati sul supporto prima del trasferimento e la confronta con l'impronta calcolata dopo il riversamento diretto.

8. COMPONENTI

8.1. COMPONENTI LOGICHE

I servizi Windows sono utilizzati per effettuare le operazioni di conservazione (creazione del PdA, ecc.) e per l'esecuzione delle attività di Virgilio (monitoraggio, ecc.). I servizi gestiti attraverso la *console* di configurazione del sistema sono i seguenti:

1) *Accettazione* - Servizio usato per inserire nuovi documenti in Virgilio: come sistemi di *input* può utilizzare *file* di testo (stile CSV con separatore o a lunghezza fissa) e/o può interfacciarsi direttamente con Archiflow (oppure con un altro Sistema documentale) attraverso l'utilizzo di un modulo specifico;
2) *Creazione PdA* - Servizio per la creazione del PdA in base a modelli predefiniti;
3) *Certificazione* - Servizio per la certificazione automatica del PdA con apposizione di firma digitale e marca temporale;
4) *Materializzazione* - Creazione delle copie fisiche in base alle regole impostate;
5) *Monitoraggio* - Servizio di monitoraggio dell'archivio digitale; pianificato periodicamente dal responsabile della manutenzione del SdC, prevede la verifica della consistenza e coerenza dei documenti;
6) *Operazioni generiche* - Servizio per la gestione delle operazioni generiche quali ad esempio la cancellazione, le richieste effettuate dal *web*, ecc.;
7) *WCF per il Web* -Servizi WCF per il web; può essere definito una volta sola per tutto l'impianto;
8) *WCF di amministrazione* - I servizi WCF di amministrazione dispongono di una serie di funzionalità per la creazione di Aziende, tipologie documentali, ecc.; può essere definito una volta sola per tutto l'impianto;
9) *WCF per i Gadget*- Espone i servizi per l'utilizzo dei Gadget di Virgilio; può essere definito una volta sola per tutto l'impianto;
10) *FTP HTTPS*- Non è un servizio Windows; viene utilizzato dal SdC per identificare la modalità di trasporto delle copie ISO sul *server web* tramite il protocollo HTTPS;
11) *Gestione PdA* - Gestisce la storicizzazione del PdA corrente delle immagini.

Tali servizi, in ambienti che utilizzano più *server*, possono essere definiti più volte in modo da parallelizzare le operazioni su entità differenti.

Le funzionalità che caratterizzano il SDC sono di seguito sintetizzate:

- verifica dei documenti in termini di leggibilità, integrità, ecc.;
- gestione del PdA di documenti;
- certificazione del PdA;
- materializzazione del PdA certificato;
- ricerca ed esibizione dei documenti;
- monitoraggio sullo stato logico e fisico del sistema;
- amministrazione e configurazione del sistema.

8.2. COMPONENTI TECNOLOGICHE

Nell'architettura di Virgilio, i servizi caratterizzanti sono interoperabili secondo una definizione formale indipendente dalla piattaforma e dalle tecnologie di sviluppo (come Java, .NET, etc.) dato che viene applicata una logica comunemente conosciuta come *Service-Oriented Architecture* (SOA). Ciò significa che ogni servizio può essere richiamato per eseguire i propri compiti senza avere conoscenza dell'applicazione chiamante e senza che l'applicazione, a sua volta, abbia conoscenza del servizio che effettivamente esegue l'operazione.

Il SOA funziona attraverso l'uso di un componente di orchestrazione, secondo il modello dell'Enterprise Service Bus, che opera nel rispetto dei principi di cooperazione applicativa basati sullo standard xml.

L'implicazione principale di un tale approccio, grazie alla possibilità di modificare in maniera semplice le modalità di interazione tra i servizi e in generale la loro combinazione (per soddisfare le esigenze dei processi che implementano), prevede che la logica di *business* sia svincolata dalla tecnologia utilizzata, per cui è possibile realizzare la separazione tra "cosa un'applicazione fa" da "come lo fa".

Un ulteriore vantaggio di un'architettura a servizi è l'integrazione immediata con altri applicativi via *web services*; in sintesi altri applicativi, indipendentemente dal linguaggio di programmazione in cui sono stati scritti e dalla piattaforma su cui sono implementati, possono utilizzare i servizi messi a disposizione attraverso l'invio tramite HTTPS di messaggi in formato xml.

L'organizzazione in servizi, interagenti tra loro e attivabili in funzione delle esigenze, permette di massimizzare anche la modularità e l'estensibilità della soluzione, ottimizzando da una parte il carico di lavoro e soddisfacendo dall'altra tutte le esigenze di amministrazione delle attività di conservazione a norma degli archivi digitali.

In particolare in Virgilio sono attivi i seguenti moduli:

- Accettazione PdV
- Generazione PdA
- Certificazione PdA
- Materializzazione PdA;
- Monitoraggio
- Gestione PdA

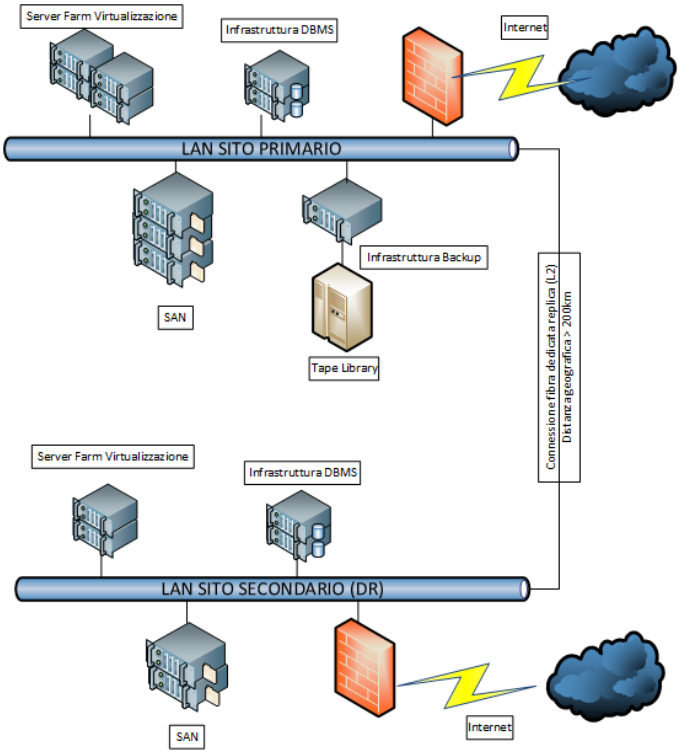

Figura 8 Infrastruttura *Disaster Recovery*

8.3. COMPONENTI FISICHE

L'architettura del SDC è stata progettata per gestire in modo ottimale la *performance* del processo di conservazione e di esibizione, applicando un approccio multi-server e tecniche di bilanciamento intelligente del carico di lavoro.

In particolare essa garantisce:

- l'estensibilità della soluzione, grazie alla possibilità di attivare solo i moduli necessari per la specifica implementazione;
- l'alta affidabilità, grazie alla possibilità di distribuire i moduli su *server* indipendenti e di clusterizzare tutti i suoi componenti;
- la scalabilità, grazie alla possibilità di distribuire i vari moduli su più *server* al crescere del carico di lavoro e di sfruttare la piena compatibilità con i più diffusi e affidabili sistemi NAS e SAN per la gestione dello *storage*.

Le diverse componenti critiche e significative ("*sensitive*") del sistema di conservazione sono isolate da altri ambienti organizzativamente, fisicamente e logicamente, in quanto organizzativamente il DSO è un settore specifico con personale dedicato; dal punto di vista logico il SDC risulta configurato su macchine dedicate, gli schemi database e le reti sono separate, la SAN è frazionata, ecc.

Per quanto riguarda l'isolamento fisico:

- gli apparati del SDC sono collocati in un'area sorvegliata, accessibile soltanto al personale autorizzato;
- il sito di *Disaster Recovery* è ospitato nei locali di un Data Center certificato, posizionato a una distanza in linea d'aria superiore a 200 km dal sito primario.

Per ulteriori dettagli si rimanda al Piano della sicurezza (in Appendice).

APPENDICE – CENNI SUL PIANO PER LA SICUREZZA

Il piano della sicurezza del sistema di conservazione si pone l'obiettivo di garantire, monitorare e controllare la sicurezza dei sistemi informativi a supporto del sistema di conservazione, minimizzando il rischio residuo, assicurando la continuità del *business* e il soddisfacimento dei requisiti relativi alla *privacy* e alla protezione dei dati personali trattati dall'organizzazione.

Il piano assicura che le informazioni siano disponibili, integre, riservate e che per i documenti informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale, l'estensione della validità temporale.

I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In questa sede si dà una descrizione sommaria degli aspetti generali del piano; per i dettagli si rimanda al documento "Piano della Sicurezza del Sistema di conservazione".

I. ASPETTI GENERALI

Le misure generali, tecniche ed organizzative, inerenti alla gestione dei documenti informatici sono in linea con quanto stabilito dalla normativa aziendale in materia di sicurezza informatica (cfr. Circolare n. 184 *Norme in materia di sicurezza informatica*), che definisce e disciplina il sistema costituito dall'insieme di norme di comportamento, assetti organizzativi, misure tecniche, metodologie e processi volti alla tutela delle risorse informatiche dell'Istituto.

Il piano della sicurezza si basa sull'analisi dei rischi a cui sono esposti i dati e i documenti trattati e rispetta le indicazioni fornite a livello nazionale dall'AgID. Nello specifico descrive:

- le misure di sicurezza relative alle componenti organizzativa, fisica, logica e infrastrutturale;
- le modalità di funzionamento del sistema di conservazione e di accesso ai documenti in esso contenuti;
- le misure specifiche adottate in materia di protezione dei dati personali, ai sensi dell'art. 32 del GDPR, e la procedura da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del GDPR.

II. POLICY DI VISIBILITÀ DEI DOCUMENTI

All'interno del sistema di conservazione sono previsti livelli differenziati di visibilità dei documenti, che variano in funzione della mansione svolta, della riservatezza dei documenti e dei dati particolari eventualmente contenuti.

III. CONTESTO NORMATIVO DI RIFERIMENTO

Circolare	Finalità
Circolare n. 184 ***Norme in materia di sicurezza informatica***	La Circolare disciplina il sistema costituito dall'insieme di norme di comportamento, assetti organizzativi, misure tecniche, metodologie e processi volti alla tutela delle risorse informatiche dell'Istituto. Si definiscono gli obiettivi, i princìpi generali, le responsabilità dei ruoli organizzativi interessati e i processi fondamentali del sistema aziendale di sicurezza informatica.
Circolare n. 257 ***Disposizioni in materia di trattamento dei dati personali***	La Circolare disciplina l'attuazione delle norme in materia di trattamento dei dati personali in Banca. La normativa stabilisce i ruoli e le connesse responsabilità nel trattamento dei dati personali, altamente personali, rientranti in categorie particolari (es. salute, orientamento sessuale) e relativi a condanne penali e reati.
Circolare n. 276 ***La tutela della riservatezza delle informazioni***	La Circolare ha l'obiettivo di favorire la consapevolezza da parte di tutto il personale del livello di riservatezza delle informazioni trattate. Prende in considerazione i due profili, strettamente connessi, relativi alla classificazione delle informazioni e ai presidi di sicurezza che ne discendono; questi ultimi vengono declinati anche con riferimento al livello di circolazione delle informazioni e ai comportamenti da assumere nel trattamento dei documenti riservati.
Circolare n. 281 ***Sistema aziendale di gestione del rischio operativo***	La Circolare disciplina il sistema adottato in Banca per la gestione del rischio operativo (*Operational Risk Management*, ORM), individuando i soggetti coinvolti e le attività da svolgere.