Commissione di Vigilanza sui Fondi Pensione

Manuale di gestione documentale della COVIP

Versione del 18 gennaio 2022

Registro delle versioni

Ver.	Autore	Ruolo	Data	Azione
1.0	Enrico Mattioni	RGD	18/01/2022	Emissione del documento

SOMMARIO

1 Principi generali

1.1 Premessa

Il presente Manuale di gestione documentale (di seguito Manuale) descrive e disciplina la gestione informatica dei documenti formati e acquisiti dalla COVIP e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Con il termine gestione documentale si intende l'insieme delle attività relative al trattamento dei documenti acquisiti o prodotti dalla COVIP idonee a garantire:

- certezza documentale;
- assegnazione alla Struttura competente e ordinata conservazione.

La certezza documentale consiste nel garantire, per ciascun documento:

- autenticità (certezza dell'autore - non ripudiabilità - e della provenienza);
- integrità (completezza e inalterabilità del documento);
- conoscenza della controparte, nei casi in cui questa sia necessaria;
- identità (attributo che caratterizza un documento in modo unico e lo distingue da altri documenti).

L'assegnazione consiste nell'attribuzione di ciascun documento alle strutture organizzative competenti per la trattazione del procedimento amministrativo o dell'affare cui il documento si riferisce.

L'ordinata conservazione consiste nelle attività volte a garantire la conservazione e il reperimento dei documenti attraverso la classificazione e la fascicolazione degli stessi.

1.1.1 Approvazione e aggiornamento del Manuale

Il Manuale è predisposto dal Responsabile della gestione documentale d'intesa con il Responsabile della conservazione e con il Responsabile per la transizione digitale. Sullo stesso è acquisito il parere del Responsabile della protezione dei dati.

Il Manuale, in sede di prima adozione, è approvato dalla Commissione (l'organo di vertice della COVIP), su proposta del Responsabile della gestione documentale (di seguito, RGD).

Il Manuale e i relativi allegati sono aggiornati direttamente dal RGD, previo parere del RPD, a seguito di:

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

Il RGD notizia la Commissione con riferimento alle modifiche di maggior rilievo.

1.1.2 Diffusione del Manuale

Il Manuale è pubblicato sul sito internet della COVIP, nella sezione “Amministrazione trasparente”.

1.2 Riferimenti normativi, acronimi e glossario

I principali riferimenti normativi considerati nella redazione del presente Manuale sono:

- Codice dei beni culturali (D.lgs. 4/2004);
- D.P.R. 445/2000 (artt. 67-69);
- CAD (artt. 29, 34, 43 e 44);
- *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall’AGID
- Codice *privacy (*Decreto Legislativo 30 giugno 2003, n.196 come modificato dal Decreto Legislativo 10 agosto 2018, n. 101).

Nell’**Appendice A** vengono riportati i riferimenti normativi di interesse per la gestione documentale.

Gli acronimi utilizzati nella redazione del presente Manuale sono i seguenti:

Sigla	Significato
AGID	Agenzia per l’Italia Digitale
AOO	Area organizzativa omogenea
BaaS	*Backup as a Service*.
CAD	Codice dell’amministrazione digitale (ultimo aggiornamento Decreto Legislativo 13 dicembre 2017, n. 217), emanato con lo scopo di assicurare e regolare la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione, nei rapporti tra amministrazione e privati e di rafforzare la digitalizzazione
COVIP	Commissione di Vigilanza sui fondi pensione
DPO	Vedi RPD
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (“General Data Protection Regulation”), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
IPA	Indice delle Pubbliche Amministrazioni
PEC	Posta elettronica certificata
PEO	Posta elettronica ordinaria
RGD	Responsabile della gestione documentale della COVIP
RCD	Responsabile della conservazione della COVIP
RPD	Responsabile della protezione dei dati personali
RTD	Responsabile della transizione al digitale
SGID	Sistema di gestione informatica dei documenti
SGSI	Sistema di gestione della sicurezza delle informazioni
UO	Unità Organizzativa

Sigla	Significato
UOP	Unità Organizzativa di Protocollo

Nell'**Appendice B** è riportato il glossario con le definizioni dei termini specialistici utilizzati nel Manuale.

2 Il modello organizzativo

2.1 Area organizzativa omogenea

Per la gestione informatica dei documenti è individuata un'unica Area Organizzativa Omogenea (AOO).

Le Unità Organizzative (UO) nelle quali si articola l'AOO sono individuate nell'atto di organizzazione delle aree e degli uffici dell'Amministrazione e sono riportate sul sito della COVIP (www.covip.it), nella sezione Amministrazione trasparente | Organizzazione | Articolazione degli uffici.

2.2 Il servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi

È istituito il servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi.

Il servizio è da intendersi come l'insieme delle attività svolte da diverse UO al fine di adempiere agli obblighi previsti dalla normativa. Esso è realizzato nel rispetto dell'attuale assetto organizzativo della COVIP.

Le principali UO di riferimento per lo svolgimento di tali compiti sono il Servizio Affari Generali e il Servizio Sistemi Informativi.

L'Unità Organizzativa Protocollante (UOP) è individuata nell'Ufficio Segreteria Generale, all'interno del Servizio Affari Generali.

In particolare, il servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi assolve ai compiti previsti dall'art. 61 del TUDA, che consistono in:

1) attribuire il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
2) garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni normative;
3) garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
4) curare che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
5) garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso;
6) autorizzare le operazioni di annullamento;
7) vigilare sull'osservanza delle disposizioni della normativa vigente in materia di gestione documentale da parte del personale autorizzato e degli incaricati.

Il RGD è preposto al suddetto servizio e definisce i profili organizzativi e operativi per l'assolvimento dei suddetti compiti, secondo quanto riportato nel presente Manuale. Il

RGD, se del caso, fornisce anche indicazioni specifiche alle singole UO ai fini dell'assolvimento dei compiti descritti.

Le singole operazioni di annullamento del protocollo sono autorizzate dal Responsabile del Servizio Affari Generali secondo le modalità previste nel **par. 6.7**.

2.3 Il Responsabile della gestione documentale

La COVIP, con delibera della Commissione del 16 luglio 2020, ha individuato quale RGD il Responsabile del Servizio Sistemi Informativi.

Al RGD sono affidati i seguenti compiti:

1) curare la gestione dei flussi documentali;
2) predisporre lo schema del Manuale di gestione dei documenti informatici e curare, una volta approvato dalla Commissione, la pubblicazione del Manuale sul sito web della COVIP;
3) assicurare la trasmissione del contenuto del pacchetto di versamento, da lui prodotto, al sistema di conservazione secondo le modalità operative definite nel Manuale di conservazione;
4) trasmettere almeno una volta all'anno al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi;
5) proporre i tempi, le modalità e le misure organizzative e tecniche per l'eliminazione dei protocolli diversi dal protocollo informatico;
6) predisporre, d'intesa con il Servizio Sistemi Informativi, il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, parallelamente alla definizione delle misure di sicurezza in tema di protezione di dati personali;
7) adottare i più opportuni strumenti di raccordo e consultazione con le altre figure coinvolte nel processo di digitalizzazione della COVIP (Responsabile per la transizione al digitale, RCD, Responsabile della prevenzione della corruzione e Responsabile per la trasparenza).

Il RGD inoltre autorizza:

- l'utilizzo del registro di emergenza;
- il trasferimento dell'archivio cartaceo presso i locali adibiti all'archivio di deposito;
- lo scarto della documentazione.

Il RGD è altresì responsabile dell'aggiornamento del presente Manuale.

Tutte le UO, pertanto, devono segnalare tempestivamente al suddetto ogni evento suscettibile di incidere sull'operatività ed efficacia del Manuale medesimo, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione dello stesso.

2.4 Il Responsabile della conservazione

La COVIP, con delibera della Commissione del 16 luglio 2020, ha individuato quale RCD un funzionario del Servizio Sistemi Informativi.

Al RCD sono affidati i seguenti compiti:

- definire e attuare le politiche complessive del sistema di conservazione e governarne la gestione con piena responsabilità ed autonomia;
- predisporre il Manuale di conservazione e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;
- assicurare che il sistema di conservazione, per quanto in esso conservato, abbia caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità;
- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tenere evidenza, in conformità alla normativa vigente;
- gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
- generare il rapporto di versamento, secondo le modalità previste dal Manuale di conservazione;
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di conservazione;
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- individuare le specifiche funzioni e competenze del processo di conservazione da affidarsi a soggetti esterni, pubblici o privati, accreditati come conservatori presso l'AGID;
- adottare i più opportuni strumenti di raccordo e consultazione con le altre figure coinvolte nel processo di digitalizzazione della COVIP (Responsabile per la transizione al digitale, RGD, Responsabile della prevenzione della corruzione e Responsabile per la trasparenza).

2.5 Ruoli e responsabilità delle UO e degli utenti

Il modello organizzativo di protocollazione adottato dalla COVIP è accentrato sia in ingresso sia in uscita: è la UOP, pertanto, che si occupa di effettuare le registrazioni di protocollo sia dei documenti in entrata sia dei documenti in uscita.

Tutti i documenti prodotti e ricevuti dall'Amministrazione sono protocollati nel Registro di protocollo ufficiale tramite il SGID e inseriti nell'archivio di protocollo.

Il SGID, oltre all'archivio relativo al protocollo, gestisce anche altri archivi e repertori informatici, rilevanti per l'attività dell'Istituzione.

Ciascuna UO (Servizio) è responsabile per la tenuta degli archivi e repertori, sia analogici sia informatici, di competenza della UO medesima e informa il RGD o un suo delegato circa eventuali criticità.

Nell'**Appendice C** sono riportate le Strutture della COVIP, così come previste nell'Organigramma istituzionale, nonché le ulteriori figure di interesse, come censite nel SGID, con le sigle utilizzate nel presente Manuale.

2.6 Le caselle PEC istituzionali

Le e-mail trasmesse e ricevute attraverso posta elettronica certificata (PEC) costituiscono il "vettore" attraverso il quale si riceve un documento informatico, che può essere allegato o incluso nel corpo stesso della e-mail.

La COVIP si è dotata di una casella PEC istituzionale che utilizza per trasmettere e ricevere documenti informatici soggetti alla registrazione di protocollo: protocollo@pec.covip.it

La casella è pubblicata sull'indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA).

La gestione della casella PEC istituzionale è affidata alla responsabilità della UOP, che procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, alla protocollazione della stessa e allo smistamento.

Sono inoltre attive altre caselle PEC, dedicate a specifiche attività che generalmente non prevedono rapporti con il pubblico. Il personale a cui è assegnata la gestione di tali caselle PEC verifica se la corrispondenza è di interesse istituzionale; in tale caso, d'accordo con il Responsabile della UO competente, la trasmette alla UOP ai fini della registrazione di protocollo.

Le caselle PEC della COVIP sono di tipo "chiuso", cioè deputate a ricevere solo i documenti informatici provenienti da altre PEC. Eventuali documenti trasmessi sulla casella PEC da caselle di posta elettronica semplici non sono considerati ricevuti.

2.7 Le caselle PEO istituzionali

Ogni dipendente della COVIP è dotato di un indirizzo e-mail istituzionale di posta elettronica ordinaria (non certificata).

Sono inoltre previste ulteriori caselle PEO:

- caselle associate a ogni UO (a livello di Servizio) e riportate sul sito della COVIP, nella sezione “Amministrazione Trasparente”;
- caselle dedicate a specifiche esigenze o legate alla specifica funzione assunta da una persona.

Di norma, le e-mail trasmesse o ricevute nelle caselle PEO non sono soggette a registrazione di protocollo, salvo quanto previsto nel **par. 6.3.2**.

2.8 Utilizzo della firma elettronica e della firma digitale

La COVIP utilizza la firma digitale per l’espletamento delle attività istituzionali e gestionali con l’obiettivo di rendere manifesta e di consentire la verifica della provenienza e l’integrità di un documento informatico o di un insieme di documenti informatici.

I titolari di firma digitale alla data di approvazione del presente Manuale sono le figure che hanno il potere di firmare atti istituzionali della COVIP a valenza esterna; si tratta, nello specifico, del Presidente, dei Commissari, del Direttore Generale, dei Direttori Centrali, dei Responsabili dei Servizi e dei Responsabili degli Uffici di amministrazione con poteri di spesa.

2.9 Conservazione della documentazione

La COVIP si è dotata di un servizio di conservazione da parte di un soggetto terzo che svolge professionalmente tali servizi.

Per maggiori informazioni circa le caratteristiche del servizio si rimanda al Manuale di conservazione della COVIP.

3 Documenti prodotti o acquisiti dalla COVIP

3.1 Tipologie di documento

La COVIP, nella sua attività, gestisce documenti sia informatici sia analogici.

I documenti informatici sono recapitati a mezzo canale telematico o altro servizi online, PEC, PEO o supporto rimovibile (quale, ad esempio, CD ROM, DVD, pen drive, ecc.) consegnato direttamente al personale della UOP.

I documenti analogici sono recapitati attraverso posta ordinaria o corriere, a mezzo posta raccomandata, per fax o con consegna diretta a mano da parte dell'interessato (o tramite persona dallo stesso delegata) al personale della UOP.

Il documento, sia esso analogico o informatico, in base allo stato di trasmissione può essere:

- in entrata;
- in uscita;
- interno.

3.1.1 Documenti in entrata

I documenti in entrata sono tutti gli atti aventi rilevanza giuridica prodotti da soggetti esterni ed acquisiti dalla COVIP nell'esercizio delle sue funzioni.

I documenti inviati dal personale della COVIP a titolo individuale e indirizzati alla COVIP medesima (ad esempio, all'Organo di vertice o al Direttore Generale) sono da considerarsi come provenienti dall'esterno e non come documenti interni.

3.1.2 Documenti in uscita

I documenti in uscita sono tutti gli atti aventi rilevanza giuridica prodotti dalla COVIP nell'esercizio delle proprie funzioni e trasmessi a soggetti esterni.

3.1.3 Documenti interni

Per documenti interni si intendono tutti gli atti prodotti all'interno della COVIP con tecnologie informatiche, che possono essere:

- di natura prevalentemente informativa;
- di natura prevalentemente giuridico-probatoria.

I documenti interni di natura informativa, quali mere comunicazioni interne scambiate tra le UO, richieste di interventi di manutenzione PC, ecc. non sono inseriti nel SGID. Di regola, lo scambio di tali documenti avviene per mezzo della posta elettronica interna.

I documenti interni di natura prevalentemente giuridico-probatorio sono quelli redatti al fine di documentare fatti, stati o qualità inerenti all'attività svolta e alle azioni amministrative intraprese, ovvero qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Tali documenti sono inseriti nel SGID e soggetti a registrazione di protocollo, ovvero soggetti a registrazione particolare.

L'**Allegato 3** riporta le tipologie di documenti interni per i quali è prevista la registrazione particolare e quelli inseriti in altri archivi.

3.2 Formati informatici ammessi

Il SGID accetta i formati indicati nell'**Allegato 5.**

L'elenco dei formati ammessi viene verificato periodicamente in relazione alle modifiche normative e tecnologiche. In tale contesto, viene valutata anche la necessità di effettuare riversamento di file; nel caso ciò si rendesse necessario si provvede al riversamento secondo quanto indicato nell'Allegato 2, par. 3.3, delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AGID.

I documenti firmati digitalmente sono memorizzati con il formato ".p7m" (CADES) o ".pdf" (PADES).

4 Protocollo informatico: registrazione e segnatura

4.1 Registrazione di protocollo

Nell'ambito dell'AOO della COVIP, il registro di protocollo è unico ed è gestito dalla UOP.

Il registro del protocollo è atto pubblico di fede privilegiata che certifica le informazioni connesse all'elenco dei protocolli registrati nell'arco di uno stesso giorno. Tale registro soggiace alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa in materia.

Il protocollo fa fede, anche con valore giuridico, dell'effettivo ricevimento e spedizione di un documento.

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e immodificabile, delle informazioni riguardanti il documento stesso (metadati).

Sono oggetto di registrazione i documenti informatici e analogici in entrata, in uscita e interni, secondo quanto precisato nei paragrafi successivi.

Ogni registrazione di protocollo è identificata da un numero e dalla data.

Il numero di protocollo è costituito da sette cifre numeriche, oltre all'indicazione dell'anno (es: 0000001/20).

La numerazione delle registrazioni di protocollo è unica e progressiva. Il registro di protocollo si rinnova ogni anno solare: inizia il 1° gennaio dal numero 1 e termina il 31 dicembre.

Ogni numero di protocollo individua un documento e gli eventuali allegati allo stesso.

La registrazione di protocollo avviene attraverso il SGDI, che garantisce l'inalterabilità dei metadati associati, registrando tutte le eventuali variazioni successive apportate agli stessi, e l'immodificabilità dei metadati per i quali la modifica non è consentita dalla normativa.

L'eventuale modifica di metadati immodificabili può avvenire solo con l'annullamento dell'intera registrazione di protocollo, secondo quanto descritto nel **paragrafo 6.7.**

I metadati relativi alla registrazione di protocollo sono riportati nell'**Allegato 4**.

4.2 Il registro giornaliero di protocollo

Il registro giornaliero di protocollo include, in modo ordinato e progressivo, l'elenco delle registrazioni di protocollo in arrivo, in partenza e interne eseguite nell'arco della giornata.

Il registro giornaliero di protocollo viene predisposto dal SGID mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica e immodificabile, in formato PDF. Considerando tale modalità di formazione, non è attualmente prevista la

sottoscrizione con firma digitale del registro giornaliero, in quanto ritenuta non necessaria.

Il registro giornaliero di protocollo viene generato e trasmesso al sistema di conservazione digitale giornalmente, di norma entro la giornata lavorativa successiva a quella di riferimento. Lo stesso viene anche salvato nel SGID, in un apposito archivio.

Il registro giornaliero di protocollo trasmesso in conservazione digitale contiene sia gli inserimenti di nuove registrazioni, sia le eventuali modifiche e gli eventuali annullamenti effettuati nel giorno di riferimento.

I dati del registro giornaliero di protocollo sono riportati nell'**Allegato 4.**

4.3 Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla loro identificazione univoca e certa.

La segnatura viene effettuata associando al documento informatico (a prescindere dal fatto che lo stesso sia nativo digitale oppure acquisito successivamente, tramite scansione) il corrispondente file della segnatura, generato automaticamente dal sistema in formato XML, predisposto secondo quanto prescritto nell'Allegato 6 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AGID.

L'operazione di segnatura di protocollo viene effettuata contemporaneamente a quella di registrazione di protocollo.

4.4 Documenti esclusi dalla registrazione di protocollo

Sono esclusi dalla registrazione di protocollo i documenti rientranti nelle tipologie di documenti di cui all'art. 53 comma 5 del D.P.R. 20 dicembre 2000, n. 445 e di seguito elencate: gazzette ufficiali; bollettini ufficiali; notiziari delle pubbliche amministrazioni; note di ricezione delle circolari e altre disposizioni; materiali statistici; atti preparatori interni; giornali e riviste; libri e materiale pubblicitario.

Sono altresì esclusi dalla registrazione di protocollo tutti i documenti soggetti a registrazione particolare, individuati nell'**Allegato 3.**

4.5 Documentazione non di pertinenza della COVIP

La documentazione analogica non di pertinenza della COVIP, nel caso in cui la busta non sia stata aperta, non viene protocollata e viene inoltrata nuovamente al mittente con la dicitura "Documentazione pervenuta per errore - non di competenza di questa Autorità".

Nel caso in cui la busta sia stata aperta per errore, il documento viene protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento

pervenuto per errore" e si inoltra al mittente apponendo sulla busta la dicitura "Documentazione pervenuta ed aperta per errore - non di competenza di questa Autorità".

Nel caso in cui pervengano sulla casella PEC istituzionale della COVIP o sui canali presidiati messaggi dal cui contenuto si rilevi con immediatezza che sono stati ricevuti erroneamente, la UOP rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Autorità".

Qualora sia la UO assegnataria a rilevare tale errore lo segnala alla UOP che provvede a restituire il documento al mittente con la medesima dicitura.

4.6 La registrazione differita (o "protocollo differito")

Nel caso di eccezionale carico di lavoro, tale da non permettere di evadere la corrispondenza ricevuta nei tempi indicati nel **par. 6.1.1** e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa risultare leso un diritto di terzi (es. partecipazione concorso), è possibile effettuare la registrazione differita di protocollo per i documenti in ingresso.

In particolare, il protocollo differito viene autorizzato dal Responsabile del Servizio Affari Generali con un atto nel quale vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata. Si applica solo ai documenti in arrivo e per tipologie omogenee, che devono essere indicate nell'atto di autorizzazione.

4.7 Il registro di emergenza

Nel caso in cui non sia possibile utilizzare il SGID, il RGD autorizza l'attivazione del registro di emergenza secondo la procedura operativa relativa all'attivazione e gestione del Registro di emergenza descritta nell'**Allegato 6**.

La data di registrazione del protocollo nel registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

La copia informatica del registro di emergenza viene conservata nel SGID, all'interno di un apposito archivio.

5 La gestione dell’archivio informatico

5.1 Categorie logiche di archivi

L’archivio della COVIP può essere logicamente distinto, a seconda del formato dei documenti che lo compongono, in informatico o analogico e, a seconda della frequenza di utilizzo della relativa documentazione, in corrente o di deposito.

L’archivio informatico è composto da tutti i documenti informatici di pertinenza della COVIP, a prescindere dal fatto che gli stessi siano o meno nativi nel formato digitale.

L’archivio analogico è composto da tutti i documenti cartacei di pertinenza della COVIP.

L’archivio corrente è il complesso dei documenti informatici e/o analogici necessari allo svolgimento delle attività in corso o, comunque, verso i quali sussista un interesse non ancora esaurito.

L’archivio di deposito è il complesso di documenti relativi a procedimenti amministrativi o affari verso i quali non sussista più un interesse di trattazione corrente, o l’interesse sia comunque sporadico e non preventivabile.

Il SGID gestisce sia l’archivio informatico corrente, secondo modalità ordinarie, sia l’archivio informatico di deposito, in maniera distinta dall’archivio corrente e con privilegi di accesso più ristretti rispetto a quest’ultimo.

L’archivio analogico corrente e, di norma, anche l’archivio analogico di deposito sono entrambi collocati presso le singole UO competenti, che sono responsabili della corretta tenuta degli stessi.

È in corso di finalizzazione un progetto volto a trasferire l’archivio analogico formatosi precedentemente all’introduzione del SGID presso una struttura esterna alla COVIP, che ne effettui il servizio professionale di gestione.

Si ha altresì in programma di riversare periodicamente, presso la suddetta struttura, l’archivio analogico che si andrà via via formando negli anni futuri.

Al fine di garantire la corretta tenuta della documentazione e favorire la ricerca in maniera agevole della stessa tutti documenti soggetti a registrazione di protocollo sono classificati e fascicolati.

5.2 Il piano di classificazione

Il piano di classificazione (o titolario) permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione.

La classificazione di un documento consiste nell’attribuire allo stesso un «codice» ricavato dal piano di classificazione, al fine di inserire stabilmente i documenti medesimi nella corretta posizione logica dell’archivio corrente.

La classificazione è obbligatoria per legge e riguarda tutti i documenti protocollati.

Il piano di classificazione adottato dalla COVIP è articolato in una struttura di tipo gerarchico basata su due livelli: titoli e classi. Il titolo rispecchia una funzione essenziale svolta dalla COVIP mentre la classe individua una funzione specifica o macro-attività nell'ambito del corrispondente titolo.

Il RGD verifica periodicamente la rispondenza del piano di classificazione alle esigenze della COVIP e procede al suo aggiornamento.

Gli aggiornamenti al piano di classificazione non sono retroattivi e si applicano pertanto ai documenti protocollati dopo la loro introduzione.

Il SGID garantisce la storicizzazione delle variazioni del piano di classificazione e la possibilità di ricostruire diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del piano vigente al momento della classificazione degli stessi.

Di norma, a un documento corrisponde un'unica voce di classificazione. È però possibile che sia necessario far corrispondere allo stesso documento più voci di classificazione. In tali casi il SGID richiede di specificare quale voce di classificazione sia da considerarsi come primaria (al riguardo, si veda **par. 6.4.7**).

La classificazione guida l'utente nell'apertura del fascicolo archivistico.

Per la consultazione del piano di classificazione della COVIP si rimanda all'**Allegato 1**.

5.3 Il piano di fascicolazione e il fascicolo archivistico

Il fascicolo archivistico rappresenta un'aggregazione omogenea e organizzata di documenti relativi allo stesso procedimento amministrativo, allo stesso affare, alla stessa attività o materia oppure alla stessa persona fisica.

La COVIP utilizza le seguenti tipologie di fascicolo archivistico:

- fascicolo per procedimento amministrativo;
- fascicolo per affare;
- fascicolo per attività o materia;
- fascicolo per persona fisica;
- fascicolo per persona giuridica.

Il fascicolo per procedimento amministrativo contiene i documenti relativi ai procedimenti amministrativi, così come indicati nella tabella pubblicata sul sito della COVIP (www.covip.it), nella sezione "Amministrazione trasparente" ai sensi dell'art. 35 del Decreto lgs. 14 marzo 2013, n. 33 (Codice della trasparenza delle PP.AA.).

Il fascicolo per affare contiene una pluralità di documenti relativi a una determinata azione istituzionale, diversa dai procedimenti amministrativi, che può prendere avvio su istanza di parte o d'ufficio e la cui conclusione può dar luogo o meno a un provvedimento finale espresso.

Il fascicolo per attività o per materia contiene una raccolta di documenti ripetitivi o a carattere meramente informativo relativi a una specifica competenza, formati o ricevuti nell'ambito di un determinato arco cronologico.

Il fascicolo per persona fisica contiene i documenti relativi a una pluralità di affari, attività e procedimenti riguardanti la persona avente un rapporto con l'Autorità.

Il fascicolo per persona giuridica contiene i documenti relativi a una pluralità di affari, attività e procedimenti riguardanti una persona giuridica avente un rapporto con l'Autorità.

Ogni voce del piano di classificazione fa riferimento a una o più categorie di fascicoli tra le tipologie sopra elencate.

Un fascicolo può essere ulteriormente suddiviso in sotto-fascicoli; ciò è utile per gestire in maniera più flessibile differenti modalità di aggregazione della documentazione.

Di norma, a un documento corrisponde un unico fascicolo. È però possibile che sia necessario inserire lo stesso documento in più fascicoli. In tale caso il SGID chiede di individuare un fascicolo come principale.

In un fascicolo archivistico è possibile inserire anche documenti che non siano stati registrati al protocollo, purché siano presenti in altri archivi del SGID.

La visibilità del fascicolo non si estende automaticamente anche alle visibilità dei singoli documenti in esso inseriti.

Ciascun fascicolo archivistico viene aperto a cura dell'UO competente, di norma, all'arrivo o alla produzione del primo documento attinente allo specifico procedimento, affare o attività.

Una volta aperto un fascicolo, tutte le UO che ricevono o producono documenti attinenti allo specifico procedimento, affare o attività devono obbligatoriamente inserirli in quello stesso fascicolo, anche se aperto da altra UO.

I metadati che caratterizzano un fascicolo archivistico sono riportati nell'**Allegato 4**.

La durata del fascicolo può essere annuale o pluriennale. In particolare, il fascicolo per procedimento amministrativo e il fascicolo per affare hanno una durata pari al procedimento o all'istruttoria di riferimento, che può durare anche più di un anno. Il fascicolo per attività o materia in genere ha una durata annuale. Il fascicolo per persona fisica o per persona giuridica può restare aperto per molti anni; i fascicoli relativi ai dipendenti dell'Autorità sono di norma chiusi al termine del rapporto di lavoro.

5.4 Il fascicolo di lavoro o complementare

Il SGID consente di ricorrere, in via aggiuntiva e opzionale, a un'ulteriore modalità di raggruppamento dei documenti (fascicolo di lavoro o complementare). La fascicolazione complementare ha lo scopo di consentire, in aderenza a specifiche prassi operative, di inserire singoli documenti, oltre che nel pertinente fascicolo archivistico, in una o più ulteriori aggregazioni omogenee autonomamente definite e strutturate.

La fascicolazione complementare dei documenti è facoltativa.

In un fascicolo complementare è possibile inserire anche documenti che non siano stati registrati al protocollo, purché siano presenti in altri archivi del SGID.

5.5 Repertori informatici e altri archivi

Il SGID inserisce tutti i documenti soggetti a registrazione di protocollo in un apposito archivio, denominato “Protocollo”.

Il Sistema consente tuttavia di gestire ulteriori archivi e/o repertori informatici. I documenti registrati negli archivi e nei repertori informatici gestiti dal SGID possono essere inseriti in fascicoli archivistici o in altre aggregazioni documentali, insieme ai documenti registrati nel protocollo.

I registri particolari vengono utilizzati al fine di inserire nel SGID atti e documenti interni la cui natura fa preferire una archiviazione separata rispetto a quella del protocollo informatico.

Gli altri archivi vengono utilizzati al fine di inserire all’interno del SGID documenti per i quali si ritiene non sia necessaria la registrazione di protocollo, quali:

- gli atti preparatori interni che non si ritiene siano da assoggettare alla registrazione di protocollo o alla registrazione particolare;
- i documenti utilizzati durante la trattazione delle pratiche, quali le sentenze giurisprudenziali;
- i documenti ricevuti o trasmessi prima dell’introduzione del SGID e che possono risultare ancora utili alla trattazione delle pratiche correnti.

I repertori e gli altri archivi attivati nel SGID sono riportati nell’**Allegato 3.**

5.6 Il piano di conservazione

Il piano di conservazione o massimario di selezione e scarto illustra i tempi oltre i quali i documenti e fascicoli possono essere scartati.

Allo stato attuale il piano di conservazione della COVIP della documentazione gestita attraverso il SGID è in fase di predisposizione e verrà definito con un successivo aggiornamento al Manuale di gestione.

5.7 Procedura di scarto

La procedura di scarto dei documenti è descritta nel Manuale di conservazione.

6 Flusso di lavorazione dei documenti

6.1 Flusso del documento informatico in arrivo

6.1.1 Registrazione, segnatura, assegnazione e smistamento dei documenti

All'arrivo di un documento, la UOP provvede alla registrazione di protocollo, inserendolo nel SGID e compilando i metadati di propria competenza, e alla conseguente segnatura.

Di norma, i documenti che arrivano nei giorni lavorativi, entro le 16:00, per le giornate dal lunedì al giovedì, ed entro le ore 12:00, per la giornata di venerdì, sono registrati nello stesso giorno in cui sono arrivati. I documenti che arrivano dopo tali orari o in giorni non lavorativi sono registrati il primo giorno lavorativo utile successivo, salvo situazioni eccezionali.

La registrazione, di norma, è effettuata in ordine cronologico di arrivo. In via eccezionale, il Direttore Generale può disporre la protocollazione immediata di documenti in entrata urgenti, nel caso in cui il carattere d'urgenza emerga dal contenuto del documento stesso.

La UOP provvede anche all'assegnazione, individuando la UO di riferimento (detta anche UO responsabile o UO competente), che rappresenta l'assegnataria principale, le eventuali altre UO destinatarie dirette e le UO destinatarie per conoscenza (cfr. par. **6.1.2**).

Il documento viene quindi predisposto per lo smistamento. In questa fase il documento non è ancora visibile alle UO destinatarie.

Il Direttore Generale, o un suo sostituto o incaricato, accede al SGID e visualizza i documenti informatici in entrata predisposti per lo smistamento.

Una volta visionati dal Direttore Generale, i documenti vengono smistati alle UO destinatarie.

Qualora il Direttore Generale riscontrasse delle anomalie nei metadati, queste vengono notificate alla UOP che provvede a correggerle.

6.1.2 Ruolo delle UO nella gestione del documento

Il documento viene sempre assegnato a una UO di riferimento; possono inoltre essere eventualmente inserite altre UO destinatarie dirette e/o per conoscenza.

L'UO di riferimento è quella alla quale è attribuita la responsabilità principale della trattazione del documento.

Le altre UO destinatarie dirette collaborano con l'UO di riferimento, secondo le modalità definite da quest'ultima.

Le UO destinatarie per conoscenza sono indicate nel caso in cui si ritenga importante che le stesse siano messe al corrente della situazione rappresentata nel documento, ma di norma non partecipano alla sua lavorazione.

Il Presidente e i Commissari non possono essere mai considerati destinatari diretti, ma sempre per conoscenza. Il Direttore Generale e i Direttori Centrali invece possono essere considerati anche assegnatari diretti (di riferimento o altri), al pari delle UO, potendo trattare alcune istruttorie direttamente in prima persona.

La UO di riferimento prende in carico il documento assegnato, inserisce la voce di classificazione (se non è già stata inserita dalla UOP, altrimenti la verifica), verifica gli altri dati inseriti ed eventualmente integra la scheda documentale valorizzando gli altri metadati di interesse.

La UO di riferimento procede quindi con la fascicolazione. I responsabili dei procedimenti amministrativi delle singole UO sono responsabili della corretta fascicolazione dei documenti relativi al procedimento medesimo.

Al momento dell'assegnazione da parte della UOP, il documento è visibile solo al Responsabile della UO ed, eventualmente, al personale della UO svolgente mansioni di segreteria indicato dal Responsabile medesimo.

Sono previsti 3 diversi modelli di smistamento:

a) il Responsabile della UO provvede direttamente alle verifiche e integrazioni sopra descritte (classificazione, fascicolazione, assegnazione delle visibilità) e smista il documento al personale interno alla UO;
b) il Responsabile della UO effettua delle verifiche preliminari e trasmette il documento al personale svolgente mansioni di segreteria della UO, il quale effettua le verifiche e integrazioni sopra descritte (classificazione, fascicolazione, assegnazione delle visibilità) e smista il documento al personale interno alla UO;
c) il documento è direttamente visibile al personale svolgente mansioni di segreteria della UO, il quale effettua le verifiche e integrazioni sopra descritte (classificazione, fascicolazione, assegnazione delle visibilità) e smista il documento al personale interno alla UO.

I documenti sono resi visibili all'interno della UO e alle altre UO secondo le modalità di trattazione e i criteri propri di ciascuna UO.

6.1.3 Modifica delle assegnazioni

In caso di assegnazione errata la UO di riferimento segnala prontamente la situazione alla UOP e alla UO che ritiene competente.

La UOP provvede direttamente alla nuova assegnazione, tranne il caso in cui la UO presunta competente non si ritenga tale; in tale caso è il Direttore Generale a disporre l'assegnazione corretta.

Il cambio di assegnazione può anche essere disposto autonomamente dal Direttore Generale.

6.1.4 Visibilità dei documenti e dei fascicoli

Oltre alle assegnazioni, il SGID consente di definire le visibilità dei documenti e dei fascicoli anche ad altre UO organizzative, che possono essere interessate ad effettuare ricerche o analisi sui documenti ricevuti in relazione alle proprie competenze, anche se non partecipano alla trattazione.

Il personale che ha la visibilità dei documenti e delle aggregazioni documentali opera avendo presente la normativa posta a protezione dei dati personali di cui al GDPR e al Codice *privacy* e nel rispetto delle specifiche istruzioni ricevute per il trattamento dei dati afferenti all'attività istituzionale svolta.

Tutti i documenti e le aggregazioni documentali presenti nel SGID sono inoltre sempre visibili a:

- Presidente;
- Commissari;
- Direttore generale.

Anche il RGD e il RC hanno la visibilità completa su tutti i documenti e le aggregazioni documentali presenti nel SGID.

Il Responsabile del Servizio AA.GG. e il personale della UOP hanno la visibilità completa su tutti i documenti registrati nell'archivio di protocollo.

I soggetti che hanno la visibilità generale hanno presenti le responsabilità che ne derivano, ivi compreso il rispetto della normativa posta a protezione dei dati personali di cui al GDPR e al Codice privacy.

6.2 Ricezione di documenti analogici

I documenti analogici possono pervenire durante l'orario di apertura della COVIP presso la sede di Piazza Augusto Imperatore, 27 – Roma.

Gli stessi vengono consegnati alla UOP, che provvede all'apertura delle buste, alla normalizzazione dei documenti e all'inserimento degli stessi nel SGID.

Ai fini dell'inserimento nel SGID, il documento analogico viene dapprima scansionato, poi completato della segnatura di protocollo e allegato alla relativa scheda documentale.

Di norma, il documento analogico, anche se composto da allegati, viene scansionato nella sua interezza e non suddiviso in più file.

L'originale cartaceo del documento sottoposto a scansione viene consegnato alle UO competenti.

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione, oppure sulle quali siano presenti timbri e date, sono trasmesse alla UO competente assieme al documento.

Ciascuna UO valuta in autonomia la possibilità di conservare le buste nel caso in cui le stesse abbiano un valore giuridico – probatorio ulteriore rispetto a quello del documento contenuto.

6.3 Ricezione di documenti informatici

La COVIP acquisisce nel SGID unicamente i documenti informatici che risultino privi di virus, non risultino danneggiati e siano nei formati ritenuti ammissibili.

Se l'intero messaggio è illeggibile e non è caricabile nel SGID, lo stesso non viene sottoposto a registrazione di protocollo.

Se invece una parte dei documenti ricevuti può essere caricata nel SGID, viene comunque predisposta la scheda documentale, nella quale viene data evidenza, nelle annotazioni, della presenza di documenti informatici per i quali è risultato impossibile caricarli nel SGID, chiarendone i motivi.

La UOP segnala la circostanza al mittente, indicando che i documenti ricevuti non possono essere trattati.

6.3.1 Ricezione di documenti informatici tramite le caselle PEC

La gestione delle PEC istituzionali è integrata nel SGID. Il Sistema consente quindi alla UOP di accedere alle singole e-mail e di selezionare quelle da registrare nel protocollo informatico.

La registrazione di una PEC (sia in arrivo sia in partenza) non permette di modificare i *file* informatici associati alla stessa.

Nel caso in cui vi siano documenti allegati al testo della PEC, la UOP decide quale, tra questi e il corpo dell'e-mail, considerare come documento principale; gli altri saranno registrati come allegati.

In particolare:

a) se il testo della PEC fornisce informazioni sul contenuto della stessa, viene considerato documento principale;
b) se il testo della PEC non fornisce informazioni di contenuto, ma è di mera trasmissione, viene considerato come allegato. Il documento principale viene individuato tra gli allegati della PEC.

6.3.2 Ricezione di documenti informatici tramite caselle PEO

Le e-mail trasmesse o ricevute da caselle PEO di norma non sono soggette a registrazione di protocollo.

Gli assegnatari della casella decidono, di volta in volta e in accordo con il Responsabile della UO competente se è necessario sottoporre il documento informatico ricevuto a registrazione di protocollo in relazione al contenuto del medesimo, valutando se il contenuto sia da considerarsi giuridicamente rilevante ai fini della trattazione.

Ai fini della protocollazione è necessario che dal documento si evinca in modo esplicito sia l'oggetto che il mittente.

Nel caso in cui sia valutato necessario effettuare la registrazione di protocollo, l'e-mail viene trasmessa alla UOP, ad una apposita casella di servizio, con la richiesta di protocollazione e, per conoscenza, al Responsabile del Servizio di appartenenza della persona che richiede la registrazione di protocollo.

Per le caselle PEO assegnate alle UO o comunque gestite dalle UO, tale richiesta viene effettuata dal Responsabile del Servizio o da una persona da lui delegata.

6.3.3 Ricezione di documenti informatici attraverso il canale telematico

È in fase di implementazione un progetto per l'acquisizione di documenti informatici trasmessi dai soggetti vigilati dalla COVIP attraverso il sito internet istituzionale (www.covip.it) e per il trasferimento automatico degli stessi nel SGID.

Il sistema di acquisizione prevede che i documenti siano registrati automaticamente nel protocollo, utilizzando le informazioni fornite dal soggetto vigilato in fase di trasmissione del documento.

L'applicativo che gestisce la trasmissione attraverso il canale telematico verifica preventivamente che i documenti informatici risultino privi di virus, non risultino danneggiati e siano nei formati ritenuti ammissibili.

6.3.4 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono pervenire su supporti removibili, in modalità diverse dalla posta elettronica e dal canale telematico (ad esempio, su supporti fisici quali CD, chiavi USB ecc.).

6.4 Casi particolari

6.4.1 Corrispondenza riservata e dati personali particolari

I documenti possono essere classificati come "pubblici", "riservati" o "riservatissimi".

In ragione del segreto di ufficio di cui all'art. 15-*quater*, comma 1, del Decreto lgs. 252/2005, i documenti ricevuti e trasmessi dalla COVIP vengono, in generale, classificati come documenti riservati. La visibilità all'interno del SGID è limitata ai soggetti appartenenti alle UO destinatarie e alle altre UO autorizzate, secondo quanto previsto nei **parr. 6.1.2.** e **6.1.4.**

In alcuni casi, tuttavia, si potrebbe rendere necessario garantire un livello di riservatezza delle informazioni più elevato (cc.dd. "riservatissimo"). In questi casi la circolarità è ristretta ulteriormente rispetto a quella ordinaria, essendo il documento visibile unicamente ai soggetti espressamente abilitati ad operare su quel documento.

Il carattere di "riservatezza" può essere attribuito anche in un momento successivo alla registrazione, consentendo di limitare la visibilità del documento nel corso del flusso di lavorazione.

Analoga circolazione limitata viene garantita per i documenti che presentano, all'interno, dati personali particolari ai sensi del GDPR.

Per entrambe le situazioni è previsto l'inserimento di uno specifico metadato associato al documento, al fine di consentire la rintracciabilità dello stesso.

6.4.2 Segnalazioni statistiche e di vigilanza

Le segnalazioni statistiche e di vigilanza che i fondi pensione trasmettono ai sensi della Circolare prot. n. 250 dell'11 gennaio 2013, e successivi aggiornamenti, e le connesse comunicazioni tecniche non sono sottoposte a registrazione di protocollo. Tutte le comunicazioni sono registrate dal sistema di gestione delle segnalazioni

INFOSTAT-COVIP fornito dalla Banca d'Italia, che ne consente l'individuazione univoca.

6.4.3 Documenti indirizzati nominalmente al personale della COVIP

La posta indirizzata nominalmente al personale della COVIP è regolarmente aperta e registrata dal personale della UOP, a meno che sulla busta non sia riportata la dicitura "personale", "riservata personale" o espressione equivalente. In questo secondo caso la corrispondenza viene consegnata in busta chiusa al destinatario che, se reputa che i documenti acquisiti debbano essere protocollati, provvede a trasmetterli alla UOP.

6.4.4 Corrispondenza di particolare rilevanza

I documenti in ingresso vengono assegnati alle UO a seconda della materia.

La corrispondenza che presenta una particolare rilevanza in considerazione del mittente, dell'oggetto, del valore economico e/o della gravità dei fatti segnalati è trasmessa per conoscenza al Presidente e/o ai Commissari, secondo quanto disposto dal Direttore Generale.

Il Direttore Generale e i Direttori Centrali di Area possono anche essere assegnatari diretti della corrispondenza.

6.4.5 Protocollazione di un numero consistente di documenti

Qualora si presenti la necessità di protocollare un numero consistente di documenti, l'UO interessata deve darne comunicazione alla UOP con congruo anticipo, al fine di concordare tempi e modi di protocollazione e di spedizione.

6.4.6 Documenti anonimi

Il documento anonimo pervenuto presso la COVIP viene sottoposto a registrazione di protocollo e di segnatura nel protocollo informatico. Nel campo riservato al "mittente" viene apposta la dicitura "anonimo".

6.4.7 Documenti informatici con oggetto multiplo

Nel caso di documenti in arrivo che riguardino argomenti ai quali corrispondono voci di classificazioni differenti, il documento viene registrato cercando di inserire nell'oggetto tutte le informazioni necessarie a comprendere i vari argomenti.

La classificazione primaria del documento riguarderà l'argomento prevalente o comunque individuato come tale e il documento sarà smistato alla UO competente sullo stesso.

Se sugli argomenti sono competenti UO differenti, il fascicolo principale sarà aperto dalla UO competente sull'argomento considerato prevalente. Le altre UO potranno comunque associare voci di classificazione secondarie al documento e inserirlo in fascicoli archivistici secondari, ovvero in fascicoli di lavoro o complementari.

Se gli argomenti determinano trattazioni differenti effettuate dalla stessa UO, si procede analogamente, individuando la classificazione primaria e quelle secondarie e, conseguentemente, il fascicolo principale e quelli secondari.

6.4.8 Certificati di malattia

I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

I certificati di malattia sono acquisiti consultando la banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati. Dopo averli visualizzati sono inseriti nel fascicolo relativo alla gestione delle presenze del personale.

6.4.9 Documenti relativi a bandi di gara

La corrispondenza relativa a bandi di gara non è aperta dalla UOP ma è consegnata direttamente in busta chiusa al Responsabile della UO che si occupa degli acquisti e dei contratti.

In caso di consegna a mano da parte del partecipante alla gara, o da persona delegata, sulla busta contenente tale documentazione la UOP appone la data e l'orario di consegna.

Se la registrazione avviene dopo l'ora fissata per la consegna o se la consegna avviene dopo la scadenza fissata dal bando di gara, nella registrazione di protocollo viene inserita anche un'annotazione del tipo: "documento pervenuto/consegnato alle ore hh.mm del giorno gg/mm/aaaa come risulta dall'indicazione riportata sulla busta". La busta viene scansionata e inserita nella scheda documentale, come allegato.

Nell'oggetto si riporta la descrizione della gara/offerta così come riportata nel bando e si inserisce la dicitura "busta chiusa".

6.4.10 Fatture elettroniche

La fattura elettronica rispetta i requisiti di formato e contenuto prescritti dal Decreto Ministeriale 3 aprile 2013, n. 55 (e successive modifiche), per la compatibilità con l'apposito Sistema di Interscambio (SdI).

In particolare, la normativa rende obbligatorio emettere fatture elettroniche nei confronti di tutte le amministrazioni pubbliche, sia per il ciclo attivo che per quello passivo.

La COVIP non accetta più fatture cartacee emesse in data pari o successiva al 31 marzo 2015, salvo per i soggetti non tenuti a rispettare l'obbligo di fatturazione elettronica (es. fornitori esteri, persone fisiche o giuridiche senza partita IVA, ONLUS).

Le fatture cartacee che avrebbero dovuto essere emesse in formato elettronico vengono comunque registrate a protocollo e la UO competente informa il fornitore di riemettere la fattura in formato elettronico. Il RPA terrà in considerazione solo la fattura elettronica ai fini del pagamento.

6.4.11 Esemplari identici

Nel caso in cui pervenga un ulteriore originale di un documento già protocollato, lo sesso viene comunque sottoposto a registrazione di protocollo. Una volta verificata la corrispondenza tra i due esemplari, inclusi gli allegati, nella registrazione di protocollo dell'esemplare da ultimo pervenuto si inserisce l'annotazione "Documento già pervenuto con prot. [nnn] del [gg.mm.aaaa]".

6.5 Flusso del documento informatico in uscita

La COVIP, per questioni di economicità, efficacia ed efficienza, privilegia la produzione di documenti informatici, firmati digitalmente, e la trasmissione dei documenti informatici tramite PEC.

Ove ciò non fosse possibile a causa dell'inesistenza di un indirizzo PEC del destinatario, i documenti sono trasmessi a un indirizzo PEO ovvero, in forma analogica, per posta convenzionale, posta raccomandata o corriere, a seconda dei casi.

L'UO che ha prodotto il documento in uscita, una volta che lo stesso è diventato definitivo, lo inoltra alla UOP per effettuare la registrazione di protocollo, indicando la voce di classificazione da utilizzare.

Di norma, la UOP registra, nello stesso giorno lavorativo in cui sono trasmessi, i documenti che pervengono, entro le 16:00, per le giornate dal lunedì al giovedì, ed entro le ore 12:00, per la giornata di venerdì, e nella giornata lavorativa successiva quelli che pervengono dopo tale orario.

La UOP prende in carico il documento e procede con la registrazione di protocollo e con la trasmissione del documento al destinatario.

La UOP provvede a notificare alla UO competente l'avvenuta registrazione di protocollo, in modo che quest'ultima possa procedere con la fascicolazione.

L'eventuale originale cartaceo del documento trasmesso viene conservato dalla UO che lo ha formato, secondo i criteri generali di gestione dell'archivio cartaceo.

6.6 Flusso del documento informatico interno

I documenti interni per i quali risulti necessario l'inserimento nel SGID, in appositi repertori o archivi, sono gestiti direttamente dalle UO che li producono, che provvedono all'inserimento degli stessi nei relativi archivi/repertori, alla compilazione dei relativi metadati e alla classificazione e fascicolazione, se prevista.

Per quanto riguarda i documenti interni rispetto ai quali risulti necessario provvedere alla registrazione di protocollo, si prevede una prima fase nella quale la UO che li ha ricevuti, una volta che gli stessi siano diventati definitivi, li inoltri alla UOP, indicando la voce di classificazione da utilizzare. La UOP prende in carico il documento e procede con la registrazione di protocollo, notificando alla UO competente l'avvenuta registrazione, in modo che quest'ultima possa procedere con la fascicolazione. In una fase successiva la registrazione e la classificazione di tali documenti potrà essere ad opera della UO che li ha prodotti.

6.7 Annullamento di una registrazione

Il Responsabile del Servizio Affari Generali autorizza l'annullamento di una registrazione di protocollo in uno dei seguenti casi:

a) errore di immissione di uno dei metadati non modificabili (cfr. **Allegato 4**);
b) documento registrato erroneamente due volte;

c) errata registrazione di un documento non soggetto a registrazione (cfr. **par. 4.4**).

Nel caso in cui si rendesse necessario provvedere all'annullamento di una registrazione per situazioni diverse da quelle sopra riportate, l'annullamento è autorizzato dal Responsabile del Servizio Affari Generali d'intesa con il RGD.

La richiesta di annullamento, così come la successiva autorizzazione, vengono effettuate attraverso uno scambio di e-mail.

La registrazione annullata rimane visibile all'interno del SGID, che mantiene anche le informazioni relative all'ora, alla data e al nominativo dell'operatore che ha effettuato l'operazione. Il Sistema evidenzia la registrazione annullata mostrandone il testo barrato e la dicitura "annullato".

Nella registrazione di protocollo annullata appaiono in forma ben visibile, in aggiunta agli elementi già indicati, anche la data, il cognome e nome dell'operatore che ha effettuato l'annullamento, con relativa motivazione.

In caso di variazione dei metadati modificabili, il SGID tiene memoria di tutte le modifiche effettuate su ciascuna registrazione, riportando nel dettaglio:

- nome dell'utente;
- data e ora;
- azione svolta (inserimento/modifica metadato/visualizzazione);
- valore del metadato modificato.

6.8 Trasferimento nel sistema di conservazione

Il RGD, o suo delegato, d'intesa con il RCD, provvede, almeno una volta all'anno, a creare i pacchetti di versamento con i fascicoli archivistici e a versarli al sistema di conservazione, secondo le regole previste nel Manuale di conservazione, avvalendosi anche di processi di automazione disponibili nel SGID.

Qualora, per determinate tipologie di procedimenti o di documenti, si rendesse necessario predisporre l'attivazione della procedura di conservazione con tempistiche particolari, il Responsabile dell'UO interessata da tale esigenza deve darne comunicazione al RGD e al RCD, al fine di valutare le modalità più idonee per darne attuazione.

7 Modalità di accesso al SGID

7.1 Accesso da parte di utenti interni

A tutti gli utenti interni (dipendenti della COVIP) è messa a disposizione una applicazione web su un sito intranet dedicato che consente l'accesso allo SGID.

Il SGID consente a ciascun utente di visualizzare unicamente la documentazione di propria competenza e di accedere alle relative schede documentali; il SGID permette inoltre la configurazione di profili di accesso differenziati al fine di fornire i privilegi per idonei a ricevere, assegnare, consultare, protocollare, classificare e fascicolare i documenti.

I livelli di autorizzazione per l'accesso dei dipendenti della COVIP al SGID sono definiti dal RGD d'intesa con il Responsabile dei Sistemi informativi e con il Responsabile di ciascun Servizio; gli stessi sono definiti in coerenza con quanto previsto nella regolamentazione adottata dalla COVIP sul trattamento dei dati personali in attuazione della normativa di tutela dei dati personali ai sensi del GDPR e del codice privacy.

Le tipologie di profili utente previste sono indicate nell'**Allegato 7.**

7.2 Accesso da parte di utenti esterni

Allo stato attuale non è consentito l'accesso diretto al SGID da parte di utenti esterni.

Laddove ne sussistano i presupposti, tuttavia, è possibile accedere alla documentazione contenuta nel SGID della COVIP secondo quanto previsto nel *Regolamento per l'esercizio del diritto di accesso ai documenti amministrativi* pubblicato nel sito della COVIP.

7.3 Interoperabilità con altre PP.AA.

L'interoperabilità del protocollo informatico indica la possibilità per il sistema di una amministrazione che riceve un messaggio di protocollo (con determinate caratteristiche) di trattare automaticamente le informazioni trasmesse dal sistema di un'amministrazione mittente, al fine di automatizzare le attività ed i processi sottostanti.

Il SGID adottato dalla COVIP consente di attivare la funzione di interoperabilità, che riguarda unicamente l'archivio di protocollo e opera attraverso messaggi PEC.

Il messaggio in uscita trasmesso attraverso questa funzione deve contenere necessariamente il documento amministrativo informatico principale (altrimenti il sistema non consente l'invio della e-mail); il sistema consente di scegliere se inviare o meno gli allegati.

Il messaggio contiene inoltre la segnatura di protocollo, predisposta automaticamente dal SGID in conformità a quanto previsto nell'Allegato 2 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AGID.

Alla segnatura di protocollo viene apposto un "sigillo elettronico qualificato" al fine di garantirne l'integrità e l'autenticità.

Il sistema consente di richiedere la conferma di ricezione del messaggio di protocollo da parte dell'amministrazione destinataria. La conferma viene memorizzata nel registro di protocollo.

Per quanto riguarda i messaggi ricevuti il SGID consente di individuarli rispetto alle altre PEC attraverso un apposito contrassegno.

Il sistema verifica la segnatura di protocollo, controllando la correttezza della firma della segnatura di protocollo, la corrispondenza dell'impronta del documento principale presente nella segnatura di protocollo e il documento principale ricevuto e, se presenti allegati, per ciascun allegato la corrispondenza dell'impronta dell'allegato presente nella segnatura di protocollo e l'allegato ricevuto.

Nel caso in cui, durante la fase di verifica, emergano anomalie, il sistema trasmette automaticamente le anomalie riscontrate. Nel caso in cui non emergano anomalie il sistema provvede alla registrazione di protocollo del messaggio e, laddove sia richiesta conferma, alla trasmissione della stessa.

In fase di archiviazione la scheda del documento viene aperta con i campi già compilati secondo quanto impostato nel file di segnatura ricevuto con il messaggio.

Se un documento ricevuto tramite la funzione di interoperabilità viene annullato, il sistema invia automaticamente via e-mail la notifica dell'annullamento all'amministrazione mittente.

Il SGID non consente l'invio di un documento annullato.

8 Piano per la sicurezza informatica del SGID

8.1 Policy di sicurezza informatica

Le politiche di sicurezza informatica applicate al SGID sono conformi alle politiche di sicurezza informatiche adottate in generale dalla COVIP per la protezione del proprio patrimonio informativo e per la gestione degli incidenti informatici.

Le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'accesso ai documenti informatici sono volte a garantire che:

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

Tali misure tengono in considerazione le esigenze derivanti dal rispetto delle norme sulla protezione dei dati personali, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del GDPR.

La definizione delle misure di sicurezza della COVIP è affidata al Servizio Sistemi informativi, che procede all'attuazione, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza adottate d'intesa con il RGD e con il Responsabile della tutela dei dati personali, per i profili di competenza.

Il riesame delle politiche di sicurezza è svolto periodicamente (di norma, annualmente) o in conseguenza del verificarsi di uno dei seguenti casi:

- variazioni tecnologiche significative;
- modifiche all'architettura informatica che potrebbero incidere sugli obiettivi o sul livello di sicurezza complessiva;
- aggiornamenti delle prescrizioni normative;
- risultati delle attività di *audit*;
- altri eventi che ne rendano necessaria la modifica.

In relazione al trattamento sui dati personali e alla sicurezza informatica, a tutto il personale sono fornite istruzioni sui comportamenti da tenere e sono previsti momenti di formazione specifici.

8.2 Architettura del SGID

Il SGID della COVIP è implementato attraverso applicativi e *database* installati nel *data center* della COVIP.

In particolare, il sistema prevede una architettura *multi-layer* costituita da 3 livelli

funzionali (strati):
- presentazione (*presentation layer*);
- applicazione (*application layer*);
- dati (*data layer*).

I diversi strati applicativi sono installati su due distinti *server*, che contengono:

- l'applicativo *software* principale, con i relativi moduli;
- i documenti (in ingresso, uscita e interni) acquisiti dal sistema nei formati digitali;
- il *database* relazionale, contenente i parametri di configurazione del sistema e i metadati associati ai singoli documenti.

I *server* sono predisposti in ambienti virtuali.

I singoli *client*, costituiti dalle postazioni degli utenti, accedono all'applicativo tramite *browser* e non necessitano di installazioni particolari, eccezion fatta per alcuni servizi e *plug-in* necessari all'attivazione di funzionalità specifiche.

I *file* dei documenti e i dati contenuti nel *database* sono accessibili da parte degli utenti solo tramite l'*application layer*.

L'accesso al *database*, oltre che alle utenze per l'amministrazione e a quella dell'applicativo, è consentito, in sola lettura, anche a utenze dedicate al RGD e al RCD, al fine di predisporre le interrogazioni utili a monitorare la funzionalità del SGID e la corretta utilizzazione dello stesso da parte delle UO.

8.3 Presidi di sicurezza

I presidi di sicurezza applicati al SGID sono volti a garantire l'integrità, la riservatezza, la disponibilità dei documenti e il non ripudio delle operazioni eseguite su di essi.

8.3.1 Presidi di sicurezza fisica

Il *data center* sul quale sono installati gli applicativi relativi al SGID è ubicato all'interno di una stanza, interamente dedicata, presso la sede della COVIP.

Sono previste misure di sicurezza di carattere generale volte a minimizzare i rischi derivanti da:

- accessi non autorizzati alla sede della COVIP;
- accessi non autorizzati alla stanza del data center;
- danneggiamenti fisici alle attrezzature.

8.3.2 Presidi di sicurezza logica sui server

I server che ospitano l'applicativo *software*, i documenti informatici e i *database* sono configurati in modo tale da consentire l'accesso esclusivo:
- all'utenza di servizio applicativa connessa al SGID;
- alle utenze amministrative del personale autorizzato a svolgere attività di manutenzione.

Gli accessi effettuati, ivi compresi quelli degli utenti amministrativi, sono tracciati con sistemi che consentono l'identificabilità dell'utente. Vengono inoltre tracciati gli accessi

al *database*. Le registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Sulle macchine che ospitano il sistema, nonché su tutti i dispositivi periferici del sistema (apparati di rete, firewall, ecc.) sono inoltre previsti meccanismi di raccolta generalizzata dei tracciamenti (*log collector*) e di analisi degli stessi (SIEM).

Tramite applicativi dedicati, le macchine sono sottoposte a periodiche scansioni per individuare eventuali vulnerabilità nel sistema. I rapporti di tali scansioni vengono archiviati e analizzati per valutare eventuali interventi migliorativi sui presidi di sicurezza.

8.3.3 Presidi di sicurezza logica dell'applicativo

L'accesso all'applicativo avviene utilizzando le credenziali di accesso al sistema informatico della COVIP; ciò consente l'univoca identificazione ed autenticazione degli utenti, anche ai fini del tracciamento delle operazioni compiute dallo stesso.

La politica di gestione della *password* è quella prevista, in via generale, per l'accesso al sistema informatico della COVIP, così come definita nella documentazione sul sistema di gestione della sicurezza dell'informazione.

L'inserimento di un utente nel SGID avviene secondo le procedure operative previste per la gestione del ciclo di vita dell'utenza, così come descritte nella documentazione sul sistema di gestione della sicurezza dell'informazione.

Il SGID consente di impostare un insieme granulare di privilegi di accesso attraverso i quali è possibile specificare dei ruoli, che definiscono in maniera dettagliata le autorizzazioni per la tipologia di utente.

I documenti non vengono mai visualizzati dagli utenti privi dei relativi diritti di accesso, neanche a fronte di una ricerca generale nell'archivio. Ulteriori restrizioni alla circolazione dei documenti possono essere assegnate nei casi in cui gli stessi abbiano un livello di riservatezza particolarmente elevato (cfr. **par. 6.4.1**). Nell'ambito della documentazione sul sistema di sicurezza delle informazioni sono inoltre predisposte delle linee guida per la classificazione delle informazioni che forniscono delle indicazioni operative agli utenti.

I profili di accesso implementati sono riportati nell'**Allegato 7.**

Al momento dell'inserimento l'utente acquisisce il ruolo di utente generico. Eventuali ruoli specifici vengono assegnati successivamente, su richiesta del Responsabile della UO di appartenenza dell'utente.

Alle utenze con ruoli amministrativi e alle utenze amministrative attivate per la gestione di funzioni informatiche di interscambio con altri sistemi applicativi si applicano i presidi di sicurezza previsti, in via generale, per situazioni analoghe.

Il SGID prevede il tracciamento permanente delle attività svolte dagli utenti, con la memorizzazione di ogni operazione eseguita sul documento informatico e sul fascicolo ("storia" del documento/fascicolo) e con la possibilità di individuarne l'autore.

L’applicativo è attivo tutti i giorni, dalle 7:00 alle 02:15. Dopo 45 minuti di inattività la sessione utente si interrompe e l’utente deve effettuare nuovamente l’autenticazione.

Il registro giornaliero di protocollo è trasmesso, di norma entro la giornata lavorativa successiva, al sistema di conservazione, garantendone l’immodificabilità del contenuto.

Il SGID ha inoltre attivato, per tutti i documenti inseriti, la funzionalità di *Document Digest Protection* la quale, tramite “impronta” (attraverso una funzione di *hash* crittografica) dei *file,* garantisce che un documento archiviato non possa essere sostituito o modificato mediante l'accesso diretto allo *storage* fisico che lo contiene.

Il SGID consente infine di attivare una funzionalità di *Advanced Document Protection* che, tramite un sistema di criptazione dei *file*, garantisce che i documenti archiviati nel sistema non possano essere consultati in modo non controllato mediante l'accesso diretto allo *storage* fisico che li contiene.

8.3.4 Presidi di sicurezza dei canali di comunicazione

I *client* e i *server* che accedono all'archivio dei documenti e delle PEC comunicano tramite protocolli sicuri (HTTPS, SMTPS, POP3S).

Il server di PEC del fornitore esterno (*provider*), di cui si avvale COVIP, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:
- verifica dell'invio e della ricezione da parte di gestori di posta elettronica certificata;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di invio, consegna e accettazione.

Come metodo di comunicazione verso l’esterno si predilige il canale PEC e l’invio di documenti informatici sottoscritti con firma digitale, al fine di attribuire in modo certo la titolarità del documento, la sua integrità la sua riservatezza e la validazione temporale.

8.4 Politica di *backup*

Con riferimento al SGID è prevista la seguente politica di *backup*:

1) Applicativo *software*
   Viene effettuato un *backup* giornaliero incrementale e uno settimanale completo della macchina virtuale che contiene il *software*, con un periodo di *retention* di 30 giorni. Il *backup* viene effettuato ricorrendo a un servizio *BaaS* (*Backup as a Service*) su piattaforma *cloud*.
2) Documenti digitali
   Viene effettuato un *backup* incrementale della macchina virtuale che contiene i documenti digitali ogni 2 ore; differenziale ogni giorno e completo ogni settimana. I *backup* incrementali hanno un periodo di *retention* di due settimane, quelli differenziali di tre mesi e il *backup* completo ha un periodo di *retention* di un anno.
3) *Database*
   Viene effettuato un *backup* incrementale 2 volte al giorno; differenziale ogni giorno e completo ogni settimana. I backup incrementali e differenziali hanno un periodo di *retention* di tre mesi. Il backup completo ha un periodo di *retention* di un anno.

Delle macchine che ospitano l'applicativo, i documenti informatici e il *database* viene effettuata copia di sicurezza in modalità *BaaS*.

8.5 Continuità operativa

Sono di seguito descritte le linee generali delle modalità di continuità operativa adottate rispetto ai vari componenti che interessano il SGID.

Applicativo

Per l'applicativo di gestione documentale è previsto un contratto di manutenzione con il fornitore.

In caso di guasto del software, la versione in uso del software può essere ripristinata tramite il backup della macchina virtuale o, qualora ciò non fosse possibile, tramite nuova installazione sulla macchina da parte del fornitore.

In assenza di specifiche inefficienze, l'aggiornamento del software è rilasciato per rispondere ad esigenze frutto di modifiche o novità in ambito normativo, per la correzione di eventuali vulnerabilità di sicurezza rilevate o per l'aggiornamento di funzioni utilizzate.

Server

In generale, l'ambiente operativo è strutturato in modo tale da garantire la continuità operativa, la sicurezza della integrità e della reperibilità dei dati anche a fronte di malfunzionamenti improvvisi delle apparecchiature utilizzate.

Il ripristino in caso di guasto viene governato da piani previsti dalle politiche di gestione in essere, tramite il recupero dei dati da *backup* aziendali pianificati: esso avviene tramite l'ultima copia del *backup* completo e tutte le copie dei *backup* incrementali fino al momento dell'interruzione.

Certification Authority

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

Dispositivo di firma digitale

Le firme digitali utilizzate nel sistema sono apposte tramite OTP su una applicazione installata sul dispositivo cellulare di servizio e/o personale. In caso di malfunzionamento del dispositivo, è possibile installare l'applicazione su un nuovo dispositivo.

L'UO preposta a gestire gli acquisti e i contratti della COVIP tiene traccia della scadenza associata a ciascuno dei dispositivi.

APPENDICE A – Riferimenti normativi

Per la redazione del Manuale di gestione documentale sono stati presi in considerazione i seguenti riferimenti normativi:

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- 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 (di seguito CAD);
- Decreto legislativo 26 agosto 2016, n. 179 – Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche;
- Decreto legislativo 13 dicembre 2017, n. 217 – Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche;
- Decreto legislativo 14 marzo 2013, n. 33 - Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del D. Lgs. 7 marzo 2005, n. 82;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del D. Lgs. 7 marzo 2005, n. 82;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del D. Lgs. 7 marzo 2005, n. 82;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata;
- Decreto del Ministero per l'innovazione e le tecnologie 2 novembre 2005 - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata;
- Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali aggiornato con decreto legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27

aprile 2016;

- “Linee guida sulla formazione, gestione e conservazione dei documenti informatici” emanate dall’AGID sul proprio sito istituzionale il 10 settembre 2020 e successivamente modificate e aggiornate;
- Regolamento (UE) n. 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016, noto come GDPR (General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, noto come Regolamento eIDAS, Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

APPENDICE B – Glossario

Di seguito si riportano le definizioni di alcuni termini tecnici utilizzati nel Manuale. Per la definizione di termini che non sono stati indicati è possibile fare riferimento all'Allegato 1 delle *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AGID.

Area organizzativa omogenea (AOO): insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.

Archivio**:** insieme omogeneo di documenti prodotti e/o ricevuti da un ente per lo svolgimento della propria attività. Con il termine archivio è da intendersi anche il locale adibito alla conservazione della documentazione memorizzata su supporto analogico.

Assegnazione**:** l'individuazione della UO competente per la trattazione del procedimento amministrativo o dell'affare.

Autenticità*:* Caratteristica in virtù della quale un oggetto (documento) deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.

Backup as a Service*:* Servizio per la fornitura in *cloud* del *backup* dei dati.

Classificazione**:** Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.

Conservatore: Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

Conservazione: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.

Copia informatica di un documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.

Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.

Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti anche interni delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (DPR n. 445/2000, art. 1, comma 1, lett. a).

Documento amministrativo informatico: Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.

Documento analogico: La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Documento elettronico: Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Documento informatico*:* Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Fascicolo informatico**:** Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

Firma elettronica: dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (cfr. articolo 3 del Regolamento eIDAS).

Firma elettronica avanzata: firma elettronica che soddisfa i requisiti di cui all'articolo 26 del Regolamento eIDAS (cfr. articolo 3 del Regolamento eIDAS).

Firma elettronica qualificata: firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (cfr. articolo 3 del Regolamento eIDAS).

Firma digitale: particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e l'altra privata correlate tra loro che consente al titolare, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Formato del documento informatico**:** modalità di rappresentazione della sequenza di *bit* che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

Funzione di hash **crittografica**: Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica (o digest) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Gestione documentale: Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.

Identificativo univoco: Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.

Immodificabilità: caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.

Impronta crittografica: Sequenza *di* bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica

Integrità*:* Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

Interoperabilità: Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.

Leggibilità: Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.

Manuale di conservazione: Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.

Metadati: Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.

Messaggio di protocollo: Elemento atomico di interesse per dare seguito allo scambio di documenti amministrativi protocollati tra AOO, anche di diverse amministrazioni (vedi anche: *interoperabilità*).

Piano di classificazione (o Titolario): Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

Piano di conservazione: Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.

Registro di protocollo Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.

Regolamento eIDAS: Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Repertorio**:** Tipo di aggregazione documentale che raccoglie documenti identici per forma e provenienza, ma difformi per contenuto, disposti in sequenza cronologica. Ciascun documento, in base a tale ordine, è identificato con un numero progressivo cui viene riconosciuta una valenza probatoria. Il repertorio può essere quindi considerato una maniera differente di organizzazione e ordinamento della documentazione e nello stesso tempo una forma differente di registrazione, parallela al registro di protocollo, prevista dall'art. 53, comma 5 del DPR n. 445/2000, che consente registrazioni particolari per determinate categorie di documenti.

Responsabile della conservazione*:* Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Responsabile della gestione documentale: Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

Responsabile della protezione dei dati personali: Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679

Responsabile del procedimento amministrativo: persona fisica incaricata dell'istruttoria e degli adempimenti necessari per portare a termine un procedimento amministrativo.

Scarto: Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.

Scheda documentale: scheda predisposta con riferimento a un documento, ai fini del suo inserimento nel SGID. Include il documento, eventuali allegati, e i metadati associati.

Sistema di gestione informatica dei documenti o SGID: Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445.

Soggetto conservatore: vedi "Conservatore".

Unità organizzativa: sottoinsieme di un'AOO costituita da un complesso di risorse umane e strumentali cui sono affidate una o più competenze omogenee e nel cui ambito i dipendenti assumono la responsabilità della gestione di procedimenti amministrativi e attività.

Validazione temporale: risultato della procedura informatica attraverso il quale si attribuiscono a uno o più documenti informatici una data e un orario opponibili a terzi.

APPENDICE C – Organigramma della COVIP e sigle delle Strutture censite nel SGID

L'organigramma della COVIP è riportato sul sito della COVIP (www.covip.it), all'interno della sezione "Amministrazione trasparente", sottosezione "L'organizzazione", pagina "Articolazione degli Uffici".

Alle Strutture previste nell'organigramma si aggiungono figure previste dalla normativa, quali il Responsabile della protezione dei dati, il Responsabile della prevenzione della corruzione e della trasparenza, Responsabile della conservazione, Responsabile della gestione documentale, Responsabile per la transizione al digitale.

Nel Manuale viene generalmente fatto riferimento alle Strutture di primo livello (Servizi), oltre che al Direttore generale e ai Direttori centrali titolari di Aree; laddove il nome non viene indicato per esteso vengono utilizzate le seguenti sigle:

Sigla	Nome esteso
DG	Direttore Generale
DC_VIG	Direttore Centrale dell'Area Vigilanza
DC_STUDI	Direttore Centrale dell'Area Studi, Statistiche e Affari Internazionali
AAGG	Servizio Affari Generali
LEG	Servizio Legale e Contenzioso
SABR	Servizio Amministrazione, Bilancio e Risorse Strumentali
SERU	Servizio Risorse Umane
SSI	Servizio Sistemi Informativi
SSS	Servizio Segnalazioni e Statistiche
STUDI	Servizio Studi e Affari Internazionali
VIG_CASSE	Servizio Vigilanza Casse Professionali
VIG_FP	Servizio Vigilanza Fondi Pensione
STAMPA	Portavoce della Commissione
RPD	Responsabile della protezione dei dati
RPC	Responsabile della prevenzione della corruzione
RPT	Responsabile della trasparenza
RCD	Responsabile della conservazione digitale
RGD	Responsabile della gestione documentale
RTD	Responsabile per la transizione al digitale

Id Titolo	TITOLO (primo livello)	Id Classe	CLASSE (secondo livello)	UO di riferimento [1]	Altre UO destinatarie dirette [1]	UO destinatarie per conoscenza [1]
1	Amministrazione generale	1.1	Atti inerenti ai Regolamenti interni della COVIP	LEG	SERU o SABR (a seconda dell'oggetto)	
		1.2	Accesso documentale	Il Servizio competente a formare l'atto richiesto ovvero a detenerlo stabilmente		
		1.3	Accesso civico semplice	RPCT	Il Servizio che detiene i dati, le informazioni o i documenti richiesti	
		1.4	Accesso civico generalizzato	Il Servizio che detiene i dati, le informazioni o i documenti richiesti		RPCT
		1.5	Gestione documentale, tenuta dell'archivio e conservazione	AAGG		
		1.6	Promozione e comunicazione	AAGG		STUDI
		1.7	Protezione dati personali	AAGG		DG LEG Servizio interessato
		1.8	Trasparenza e anticorruzione	AAGG		DG LEG
2	Organi di governo, collegiali e consultivi	2.1	Commissione (Organo di vertice)	AAGG/SERU		DG
		2.2	Presidente	AAGG/SERU		Diretto interessato
		2.3	Commissari	AAGG/SERU		Diretto interessato
		2.4	Direttore generale	AAGG/SERU		Diretto interessato
		2.5	Collegio dei revisori dei conti	AAGG/SERU		Diretto interessato
		2.6	Comitati tecnici			
3	Rapporti istituzionali e con l'esterno	3.1	Rapporti con Autorità estere e organismi internazionali	STUDI		
		3.2	Altra corrispondenza con Ministeri	Servizio competente in relazione all'oggetto		AAGG LEG (qualora non sia il Servizio competente in relazione all'oggetto)
		3.3	Altra corrispondenza con ulteriori Enti	Servizio competente in relazione all'oggetto		AAGG LEG (qualora non sia il Servizio competente in relazione all'oggetto)
		3.4	Relazioni con il pubblico	URP		

Id Titolo	TITOLO (primo livello)	Id Classe	CLASSE (secondo livello)	UO di riferimento [1]	Altre UO destinatarie dirette [1]	UO destinatarie per conoscenza [1]
		3.5	Convegni, eventi e attività di rappresentanza	AAGG		STUDI
4	Attività di regolamentazione	4.1	Collaborazione sulla normativa primaria e sulla normativa ministeriale di attuazione	LEG	VIG_FP / VIG_CASSE (a seconda della materia)	
		4.2	Collaborazione sull'attività regolatoria di altre Autorità	LEG	VIG_FP	
		4.3	Regolamentazione COVIP sui soggetti vigilati	LEG	VIG_FP	
		4.4	Interpretazione normativa sui fondi pensione e sui PEPP	LEG	VIG_FP	
		4.5	Interpretazione normativa sulle Casse di previdenza	LEG	VIG_CASSE	
		4.6	Analisi e verifica dell'impatto della regolamentazione	LEG		
		4.7	Attività di autoregolamentazione dei fondi pensione	LEG	VIG_FP	
		4.8	Attività di autoregolamentazione delle Casse	LEG	VIG_CASSE	
5	Attività legale e contenziosa	5.1	Contenzioso	LEG		VIG_FP, VIG_CASSE, SABR, SERU (a seconda dell'oggetto), solo per l'atto introduttivo del contenzioso
		5.2	Procedimenti sanzionatori concernenti i fondi pensione	LEG	VIG_FONDI	
		5.3	Segnalazioni all'autorità giudiziaria su questioni riguardanti i fondi pensione e le Casse di previdenza	LEG	VIG_FONDI / VIG_CASSE (a seconda dell'oggetto)	
		5.4	Azioni legali (non ancora di contenzioso)	LEG	VIG_FP, VIG_CASSE, SABR, SERU (a seconda dell'oggetto)	
6	Segnalazioni statistiche e di vigilanza	6.1	Regolamentazione manuale delle segnalazioni dei fondi pensione	SSS	VIG_FONDI	
		6.2	Regolamentazione manuale delle segnalazioni delle casse	SSS	VIG_CASSE	
		6.3	Profili tecnico/operativi sulle segnalazioni statistiche e di vigilanza	SSS		VIG_FONDI o Casse, secondo argomento
		6.4	Richieste di accreditamento per segnalazioni statistiche e di vigilanza	SSS		VIG_FONDI o Casse, secondo argomento
7	Attività di studi e statistiche	7.1	Attività di ricerca, rapporti con studiosi e istituti di ricerca	STUDI		
		7.2	Rilevazioni statistiche e questionari	SSS	VIG_FP (in relazione all'argomento)	STUDI (in relazione all'argomento)
		7.3	Produzione statistica	SSS	STUDI	
8	Risorse umane	8.1	Concorsi pubblici, selezioni e assunzioni	SERU		
		8.2	Carriera e stato giuridico	SERU		
		8.3	Incarichi al personale	SERU		
		8.4	Trattamento economico	SERU		
		8.5	Trattamento fiscale, previdenziale e assistenziale	SERU		

Id Titolo	TITOLO (primo livello)	Id Classe	CLASSE (secondo livello)	UO di riferimento [1]	Altre UO destinatarie dirette [1]	UO destinatarie per conoscenza [1]
		8.6	Assenze	SERU		
		8.7	Istanze e comunicazioni dei dipendenti ed ex dipendenti	SERU		
		8.8	Valutazione dipendenti e procedimenti disciplinari	SERU		
		8.9	Relazioni sindacali	SERU		
		8.10	Formazione e aggiornamento professionale	SERU		
		8.11	Cessazione del rapporto di lavoro	SERU		
		8.12	Personale non dipendente	SERU		
9	Risorse finanziarie	9.1	Programmazione e rendiconto generale	SABR		
		9.2	Gestione del bilancio	SABR		
		9.3	Fonti di finanziamento - gestione delle entrate e della spesa	SABR		
		9.4	Tesoreria, cassa e istituti di credito	SABR		
		9.5	Contributi per partecipazione a organismi nazionali e internazionali	STUDI	SABR	
		9.6	Imposte, tasse, ritenute prevedenziali	SABR		
10	Risorse strumentali e acquisti	10.1	Gestione della sede	SABR		
		10.2	Acquisizione e gestione di beni e servizi	SABR		
		10.3	Sicurezza dei luoghi di lavoro	SABR		
		10.4	Manutenzione ordinaria e straordinaria	SABR		
		10.5	Funzionamento uffici	SABR		
11	Vigilanza sui fondi pensione	11.1	Autorizzazioni e approvazioni	VIG_FONDI		
		11.2	Operazioni sui fondi pensione	VIG_FONDI		
		11.3	Vigilanza cartolare su profili di informativa dei fondi pensione (trasparenza)	VIG_FONDI		

Id Titolo	TITOLO (primo livello)	Id Classe	CLASSE (secondo livello)	UO di riferimento [1]	Altre UO destinatarie dirette [1]	UO destinatarie per conoscenza [1]
		11.4	Vigilanza cartolare su profili finanziari e attuariali dei fondi pensione	VIG_FONDI		
		11.5	Vigilanza cartolare su profili ordinamentali e organizzativi dei fondi pensione, attività di assessment e verifiche interne	VIG_FONDI		
		11.6	Richiesta di informazioni ai fondi pensione e interventi di vigilanza	VIG_FONDI		
		11.7	Attività ispettiva su fondi pensione	VIG_FONDI		
		11.8	Attività trasfrontaliera dei fondi pensione	STUDI/VIG_FONDI (a seconda della fase del processo)	VIG_FONDI/STUDI (a seconda della fase del processo)	
		11.9	Richieste da parte di fondi pensione	VIG_FONDI		
		11.10	Segnalazioni da parte di iscritti (esposti e altre richieste)	VIG_FONDI		
		11.11	Corrispondenza con Ministero del lavoro e delle politiche sociali su singoli fondi pensione	VIG_FONDI	LEG (limitatamente alle interrogazioni parlamentari e agli altri atti del sindacato ispettivo del Parlamento)	
		11.12	Corrispondenza con altri Ministeri e Istituzioni su singoli fondi pensione	VIG_FONDI		
12	Vigilanza sulle Casse professionali	12.1	Attività di vigilanza cartolare sulle Casse	VIG_CASSE		
		12.2	Attività ispettiva sulle Casse	VIG_CASSE		
		12.3	Richiesta di informazioni alle Casse	VIG_CASSE		
		12.4	Richiesta da parte delle Casse	VIG_CASSE		
		12.5	Segnalazioni da parte di iscritti (esposti e altre richieste)	VIG_CASSE		
		12.6	Corrispondenza con Ministero del lavoro e delle politiche sociali sulle singole Casse di previdenza	VIG_CASSE	LEG (limitatamente alle interrogazioni parlamentari e agli altri atti del sindacato ispettivo del Parlamento)	
		12.7	Corrispondenza con altri Ministeri e altre Istituzioni sulle singole Casse di previdenza	VIG_CASSE		
13	Sistema informativo, sicurezza dell'informazione e sistema informatico	13.1	Pianificazione, programmazione e sviluppo dei sistemi informatici	SSI		
		13.2	Gestione e manutenzione dei sistemi informatici	SSI		
		13.3	Sicurezza dell'informazione	SSI		
		13.4	Gestione del portale WEB e supporto agli utenti esterni	SSI		
14	Gestione Albo fondi e Registro delle persone giuridiche	14.1	Gestione Albo fondi pensione	VIG_FONDI	AAGG	SSS
		14.2	Rilascio certicazioni di iscrizione Albo	AAGG		
		14.3	Rilascio certicazioni relative al Registro delle persone giuridiche	AAGG		
		14.4	Variazione Registro delle persone giuridiche	AAGG		VIG_FONDI

Id Titolo	TITOLO (primo livello)	Id Classe	CLASSE (secondo livello)	UO di riferimento (1)	Altre UO destinatarie dirette (1)	UO destinatarie per conoscenza (1)

(1) La spiegazione delle sigle utilizzate è riportata nell'Appendice 3 del Manuale di Gestione Documentale

Manuale di gestione documentale della COVIP

Allegato 2

Piano di conservazione

Allo stato attuale il piano di conservazione della COVIP della documentazione gestita attraverso il SGID è in fase di predisposizione e verrà definito con un successivo aggiornamento al Manuale di gestione.

Allegato 3

Documenti interni, registri particolari e altri archivi

Alla data di redazione del Manuale di gestione documentale della COVIP si prevede di attivare i seguenti repertori relativi a documenti assoggettati a registrazione particolare, separata dal protocollo principale:

- Pareristica interna
- Comitato Irregolarità
- Ordini di servizio
- OdG riunioni Commissione
- Verbali riunioni di Commissione
- Relazioni per la Commissione
- Delibere della Commissione
- Provvedimenti di urgenza
- Note per il DG
- Rapporti Ispettivi Fondi pensione
- Rapporti Ispettivi Casse
- Registro di protocollo di emergenza

Gli altri documenti interni aventi natura prevalentemente giuridico-probatorio sono registrati nel protocollo informatico.

Sono state inoltre individuate alcune ulteriori tipologie di documenti, non soggette a registrazione di protocollo e per le quali si è ravvisata comunque l'opportunità di inserirle in appositi archivi del SGID.

Si tratta, ad esempio, di:

- Certificati malattia dipendenti
- Schede di valutazione dei dipendenti
- Regolamentazione interna COVIP
- Manuale di gestione documentale e di conservazione
- Infrastruttura informatica
- Sicurezza informatica
- Rapporti di incidente informatico
- Verbali del Security Board
- Piani triennali dell'informatica della COVIP
- Misure Minime Agid

Manuale di gestione documentale della COVIP

Allegato 4

Informazioni da inserire in fase di registrazione e ulteriori metadati

Nel presente allegato, nei paragrafi di seguito indicati, vengono riportati i dati che vengono visualizzati e/o richiesti dal SGID in fase di predisposizione della scheda documentale o della scheda di fascicolazione:

a) Documenti in entrata;
b) Documenti in uscita;
c) Documenti interni;
d) Repertori – dati comuni;
e) Repertori – dati specifici;
f) Fascicoli;
g) Registro giornaliero di protocollo.

La piattaforma informatica che gestisce il SGID della COVIP provvede a inserire gli ulteriori metadati previsti nell'Allegato 5 delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AGID.

Il paragrafo *g)* riporta infine i metadati relativi al registro giornaliero di protocollo.

a) Documenti in entrata

Il SGID, in fase di predisposizione della scheda documentale, visualizza e/o richiede le seguenti informazioni:

Metadato	Obbligatorio	Immodificabile	Compilazione
Numero progressivo di protocollo	√	√	SGID
Data di protocollo	√	√	SGID
Unità organizzativa protocollante	√	√	SGID
Canale di trasmissione	√		Operatore
Tipologia documentale	√		Operatore
Mittente	√	√	Operatore
Oggetto	√	√	Operatore
Numero protocollo mittente (1)	√	√	Operatore
Data protocollo mittente (1)	√	√	Operatore
Documento principale	√		Operatore
Nome file 2ocument principale			SGID
Allegati			Operatore
Descrizione allegati			Operatore
UO destinataria diretta	√		Operatore
Altre UO destinatarie dirette			Operatore
UO destinatarie per conoscenza			Operatore
Voce di classificazione	√		Operatore
Codice ente			Operatore
Codice fondo			Operatore
Livello di riservatezza			Operatore
Privacy			Operatore
Note			Operatore
Visibilità (Utenti/Gruppi/UO)	√		Operatore
Stato conservazione			SGID

(1) Nel caso in cui sia presente nel documento ricevuto

b) Documenti in uscita

Il SGID, in fase di predisposizione della scheda documentale, visualizza e/o richiede le seguenti informazioni:

Metadato	Obbligatorio	Immodificabile	Compilazione
Numero progressivo di protocollo	√	√	SGID
Data di protocollo	√	√	SGID
Unità organizzativa protocollante	√	√	SGID
Canale di trasmissione	√		Operatore
Tipologia documentale	√		Operatore
Destinatario	√	√	Operatore
Oggetto	√	√	Operatore
Documento principale	√		Operatore
Nome file 3ocument principale			SGID
Allegati			Operatore
Descrizione allegati			Operatore
UO di riferimento	√		Operatore
Voce di classificazione	√		Operatore
Codice ente			Operatore
Codice fondo			Operatore
Livello di riservatezza			Operatore
Privacy			Operatore
Note			Operatore
Visibilità (Utenti/Gruppi/UO)	√		Operatore
Stato conservazione			SGID

c) Documenti interni

Il SGID, in fase di predisposizione della scheda documentale, visualizza e/o richiede le seguenti informazioni:

Metadato	Obbligatorio	Immodificabile	Compilazione
Numero progressivo di protocollo	√	√	SGID
Data di protocollo	√	√	SGID
Unità organizzativa protocollante	√	√	SGID
Tipologia documentale	√		Operatore
Oggetto	√	√	Operatore
Documento principale	√		Operatore
Nome file 4ocument principale			SGID
Allegati			Operatore
Descrizione allegati			Operatore
UO destinataria diretta	√		Operatore
Altre UO destinatarie dirette			Operatore
UO destinatarie per conoscenza			Operatore
Voce di classificazione	√		Operatore
Codice ente			Operatore
Codice fondo			Operatore
Livello di riservatezza			Operatore
Privacy			Operatore
Note			Operatore
Visibilità (Utenti/Gruppi/UO)	√		Operatore
Stato conservazione			SGID

d) Repertori – dati comuni

Il SGID, in fase di predisposizione della scheda documentale, per tutti i repertori visualizza e/o richiede le seguenti informazioni:

Metadato	Obbligatorio	Immodificabile	Compilazione
Numero progressivo di registro	√	√	SGID
Data di registrazione	√	√	SGID
Unità organizzativa registrante	√	√	SGID
Tipologia documentale	√		Operatore
Autore	√		Operatore
UO di riferimento	√		Operatore
Oggetto	√	√	Operatore
Documento principale	√		Operatore
Nome file d5ocumento principale			SGID
Allegati			Operatore
Descrizione allegati			Operatore
Voce di classificazione	√		Operatore
Livello di riservatezza			Operatore
Privacy			Operatore
Note			Operatore
Visibilità (Utenti/Gruppi/UO)	√		Operatore
Stato conservazione			SGID

e) Repertori – dati specifici

Il SGID, in fase di predisposizione della scheda documentale, richiede ulteriori informazioni specifiche in relazione alle caratteristiche dei documenti ai quali sono dedicati i singoli repertori.

f) Fascicoli

Il SGID, in fase di creazione di un nuovo fascicoli, richiede e/o visualizza le seguenti informazioni:

Metadato	Obbligatorio	Immodificabile	Compilazione
Tipo fascicolo	√	√	Operatore
Codice fascicolo	√	√	SGID
Anno	√	√	SGID
Data di apertura	√	√	SGID
Data di chiusura	√		SGID
Oggetto	√		Operatore
Descrizione			Operatore
Note			Operatore
Voci d'indice	√		Operatore
Soggetto			Operatore
Responsabile			Operatore
UO Responsabile	√		Operatore
UO Assegnataria			Operatore
Tipo visibilità	√		Operatore
Visibilità (Utenti/Gruppi/UO)	√		Operatore
Stato archiviazione	√	√	SGID
UO Produttrice	√		Operatore
Ubicazione			Operatore
Stato conservazione			Operatore
Anni di conservazione archivio corrente (1)	√		Operatore
Anni di conservazione archivio deposito (1)	√		Operatore
Data di invio in conservazione (1)	√	√	SGID
Codice univoco versamento (1)	√	√	SGID

(1) Per i fascicoli per i quali è obbligatorio la conservazione

Gli ulteriori metadati previsti nell'Allegato 5 delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* emanate dall'AGID sono inseriti automaticamente dalla piattaforma informatica che gestisce il SGID della COVIP.

h) Metadati del registro giornaliero di protocollo

Il registro giornaliero di protocollo trasmesso in conservazione contiene almeno le seguenti informazioni:

- Archivio
- Tipo Documento
- Nr. Protocollo
- Data Protocollo
- Nr. Protocollo Mittente
- Data Protocollo Mittente
- Canale di Trasmissione
- Corrispondente
- Tipo corrispondente (Mittente/Destinatario)
- Oggetto
- Impronta
- Annullato

L'elenco completo dei metadati trasmessi al sistema di conservazione è riportato nel Manuale di conservazione della COVIP.

Allegato 5

Formati informatici ammessi dal SGID

Il SGID della COVIP accetta i seguenti formati

- PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000;
- PDF/A (PDF/Archiving), è un profilo del formato PDF creato per rispondere alla necessità di conservazione a lungo termine dei documenti elettronici (estensione .pdf);
- TIFF (Tagged Image File Format), formato immagine di tipo raster sviluppato da Aldus Corporation acquistata in seguito da Adobe (estensione .tif);
- JPG (Joint Photographic Experts Group), è il formato più utilizzato per la memorizzazione di fotografie, il suo impiego va valutato in funzione del tipo di documento da conservare poiché può comportare una perdita di qualità dell'immagine originale (estensioni .jpg, .jpeg);
- OOXML (Office open xml), formato sviluppato dalla versione 2007 della suite Office di Microsoft (estensioni .docx, .xlsx, .pptx);
- ODF (Open Document Format) è uno standard aperto, basato sul linguaggio XML sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni (estensioni .ods, .odp,.odg, .odb);
- XML (Extensible Markup Language), è un formato di testo flessibile derivato da SGML (ISO 8879); su tale formato si basano numerosi linguaggi standard utilizzati in diversi ambiti applicativi (estensione .xml);
- TXT (Text Plain Text) quale formato per i documenti a prevalente contenuto testuale (estensione .txt);
- EML, formato di file sviluppato da Microsoft per i propri client di posta elettronica: Outlook e Outlook Express. All'interno di un file EML viene archiviato un messaggio di posta elettronica preservandone la formattazione HTML originale e la relativa intestazione. Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME.

Il SGID accetta inoltre i certificati elettronici (.CER, .CRT, .PEM), le chiavi crittografiche (.pkix, .pem), le marcature temporali elettroniche (.TSR, .TSD, .TST), le impronte crittografiche (.sha1, .sha2, .md5, …), i formati previsti per le firme e i sigilli elettronici avanzati, quali le buste crittografiche XAdES (.xml), i formati CAdES (.P7M, .P7S), PAdES (.PDF) e i contenitori ASiC (.ZIP).

Manuale di gestione documentale della COVIP

Allegato 6

Procedura per l'attivazione del Registro di emergenza

1. Nel caso in cui la UOP verifichi l'impossibilità ad operare con il SGID, la stessa avverte immediatamente il Servizio Sistemi Informativi e, per conoscenza, il Responsabile della gestione documentale e il Responsabile del Servizio Affari Generali.
2. Nel caso in cui il Servizio Sistemi Informativi ritenga che la problematica si possa risolvere in tempi brevi, e comunque non oltre una giornata lavorativa, avverte di tale possibilità la UOP e, per conoscenza, il Responsabile della gestione documentale e il Responsabile del Servizio Affari Generali, fornendo una stima dei tempi di ripristino. Il Responsabile della gestione documentale, se valuta che sia comunque necessario attivare il registro di emergenza, procede secondo quanto previsto a partire dal passo n. 4.
3. Nel caso in cui il Servizio Sistemi Informativi ritenga che la problematica non possa risolversi in tempi brevi, ovvero si renda conto in fase di risoluzione che i tempi di ripristino del SGID vadano oltre quanto preventivato al passo n. 2, segnala la situazione al Responsabile della gestione documentale e, per conoscenza, al Responsabile del Servizio Affari Generali, chiarendo le problematiche che non consentono un ripristino tempestivo del SGID e fornendo una stima dei tempi di ripristino.
4. Il Responsabile della gestione documentale, valutate le problematiche segnalate dal Servizio Sistemi Informativi, autorizza l'attivazione del registro di emergenza trasmettendo via e-mail al Responsabile del Servizio Affari Generali il modulo di autorizzazione di cui al presente Allegato, opportunamente compilato e firmato.
5. La UOP utilizza il fax simile del registro di emergenza di cui al presente Allegato per riportare tutte le informazioni relative all'attivazione del registro di emergenza e le relative registrazioni di protocollo. Qualora non sia possibile utilizzare la versione informatica del fax simile, la UOP predispone e utilizza una versione analogica che verrà siglata in ogni pagina dal Responsabile del Servizio Affari Generali.
6. In particolare, sulla copertina del registro di emergenza la UOP riporta la causa, la data e l'ora di inizio dell'interruzione. La UOP inserisce nel registro di emergenza, per ogni documento, un numero progressivo che garantisce, anche a seguito di successive interruzioni, l'identificazione univoca dei documenti registrati.
7. Il Servizio Sistemi Informativi, non appena abbia ripristinato le funzionalità del SGID e ne abbia verificato il corretto funzionamento, trasmette una e-mail al Responsabile della gestione documentale e, per conoscenza, al Responsabile del Servizio Affari Generali, per segnalare la risoluzione della problematica.
8. La UOP inserisce, sulla copertina del registro di emergenza, la data e l'ora del ripristino della funzionalità del SGID, il numero delle registrazioni effettuate per ciascun giorno di interruzione e le altre informazioni ivi previste.
9. La UOP predispone una copia in formato PDF del registro di emergenza (provvedendo a una scansione dello stesso nel caso in cui sia stato necessario ricorrere a una versione analogica).
10. Il Responsabile della gestione documentale e il Responsabile del Servizio Affari Generali, verificate le informazioni inserite dalla UOP, firmano digitalmente il registro di emergenza; il Responsabile della gestione documentale avverte la UOP che può procedere all'inserimento nel SGID delle informazioni relative ai documenti protocollati in emergenza.
11. La UOP provvede a inserire nel SGID le informazioni relative ai documenti protocollati in emergenza senza ingiustificato ritardo. Per ogni registrazione riversata dal registro di

emergenza al SGID il sistema attribuisce il numero di protocollo del registro ufficiale, continuando la numerazione progressiva raggiunta al momento dell'interruzione del servizio. La UOP provvede ad associare a tale registrazione anche il numero di protocollo e la data di registrazione indicati in fase di emergenza, nel campo "Oggetto", in modo da mantenere stabilmente la correlazione tra il numero usato nel registro di emergenza e quello del registro di protocollo generale.

Le caselle e-mail da utilizzare per le suddette comunicazioni sono:

- per le comunicazioni da e verso il Servizio Sistemi Informativi l'apposita casella e-mail interna di supporto, adibita a ricevere tutte le comunicazioni relative a problematiche connesse con il SGID;
- per le comunicazioni da e verso il Responsabile della gestione documentale, l'apposita casella e-mail ordinaria interna allo stesso dedicata;
- per le comunicazioni da e verso il Responsabile del Servizio Affari Generali, la casella e-mail ordinaria.

La copia informatica del registro di emergenza viene conservata nel SGID, all'interno di un apposito archivio.

Allegato 6a
Schema di autorizzazione all'utilizzo del Registro di emergenza

Al Responsabile del Servizio AA.GG.
Sede

Oggetto: Autorizzazione all'utilizzo del Registro di emergenza num. ___ - anno ____

Il sottoscritto _____ , in qualità di Responsabile della gestione documentale, ha appurato che allo stato attuale non è possibile utilizzare correttamente le funzionalità di registrazione di protocollo informatico della piattaforma che implementa il Sistema di gestione documentale informatico della COVIP per i seguenti motivi:

_____
_____
_____
_____

Ciò premesso, il sottoscritto, considerato che il ripristino delle funzionalità della piattaforma non è previsto prima di ____ ore, autorizza l'Unità Operativa di Protocollo ad effettuare le operazioni di registrazione di protocollo sul registro di emergenza, da predisporre sulla base del fac-simile allegato al Manuale di gestione documentale e che può essere gestito anche utilizzando strumenti informatici, laddove ciò sia possibile.

L'autorizzazione resta valida fintanto che il Servizio Sistemi Informativi non avrà comunicato il ripristino e la verifica del corretto funzionamento delle suddette funzionalità.

Il sottoscritto chiede altresì al Responsabile del Servizio AA.GG. di appurare che, in sede di ripristino, venga effettuata associazione tra il numero di protocollo del registro di emergenza e il numero di protocollo del registro generale.

Roma, __/__/____

Il Responsabile
della gestione documentale

_____

Mod. 6a/MGD

FRONTESPIZIO

Autorizzazione n.	x del aaaa	(1)
Causa interruzione		(2)
Data e ora inizio interruzione		
Data e ora ripristino		
N. di registrazioni effettuate		
Dal numero		
Al numero		

N. di registrazioni effettuate il	__/__/____	
N. di registrazioni effettuate il	__/__/____	

Il Responsabile della gestione documentale

visto: Il Responsabile del Servizio Affari Generali

Data: __/__/____

(1) Indicare numero/anno

(2) Riportare una sintetica descrizione delle cause che hanno determinato l'interruzione delle registrazioni informatiche

N. Prot. di emergenza	Data prot. di emergenza	Data Arrivo	Tipo (E/U/I)	Mittente/Destinatario	Oggetto	Canale di trasmissione	N. Protocollo mittente	Data protocollo mittente	UO di riferimento	Altre UO destinatarie	UO destinatarie per conoscenza

Manuale di gestione documentale della COVIP

Allegato 7

Ruoli e categorie di utenti

Nel SGID della COVIP ogni utente può essere definito, in base al livello di accesso, come:

Supervisore: Utente che ha poteri generali sulla configurazione e ha la visibilità completa di tutti gli oggetti documentali del sistema, quali: schede, documenti, allegati, fascicoli, registri, ecc. Non compare nella lista dei destinatari e non può ricevere documenti. L'utente supervisore può essere configurato con una cassetta PEO in uscita di default: il suo indirizzo verrà utilizzato per inviare le notifiche per le PEC, per le mail di interoperabilità e per le Fatture elettroniche.

Amministratore: Diversamente da un utente, ha i diritti del Supervisore che riguardano la configurazione del sistema (può impostare organigramma, volumi, tipi documenti, archivi…) ma non può cercare, inserire, smistare documenti.

Utente a visibilità completa: Utente con la visibilità in lettura e scrittura su tutti i documenti, anche su quelli che non gli sono stati inviati o che non sono stati inviati al suo ufficio.

Utente generico: Utente con i diritti che gli sono stati assegnati dal Supervisore o da chi ha il diritto di gestione dell'organigramma.

Utente Amministratore locale: Utente generico con in più il diritto per Gestire organigrammi: avrà la possibilità di gestire un ramo di organigramma, come impostato dal Supervisore. Non avrà, però, competenza e nemmeno visibilità sugli utenti e sugli uffici gestiti da altri Amministratori.

Il ruolo di Supervisore è attribuito al personale che svolge attività di amministrazione tecnica della piattaforma di gestione del SGID; il ruolo di utente a visibilità completa è assegnato al Responsabile della gestione documentale e al Responsabile della conservazione digitale.

Tutti gli altri utenti sono impostati come utenti generici, ai quali tuttavia possono essere attribuiti differenti privilegi in relazione al ruolo svolto.

Allo stato attuale sono previste tre categorie di utenti con privilegi differenti:

1) Utente di protocollo, con i privilegi necessari per effettuare le registrazioni di protocollo;
2) Utente collaboratore, con i privilegi necessari per gestire i fascicoli e modificare i metadati delle schede documentali
3) Utente generico, con i privilegi di visualizzazione dei documenti di competenza e di accesso alle relative schede documentali.