



AUTORITÀ
NAZIONALE
ANTICORRUZIONE

Manuale della Gestione Documentale

20 ottobre 2025

SOMMARIO

DATI DEL DOCUMENTO.....	6
1. PRINCIPI GENERALI ED ORGANIZZATIVI.....	9
1.1 Premesse	9
1.2 Ambito di applicazione del manuale	9
1.3 Riferimenti normativi.....	10
1.4 Caratterizzazione dell'Area Organizzativa Omogenea	12
1.5 Modello organizzativo del Servizio di Protocollo.....	12
1.6 Servizio per la gestione informatica del protocollo	13
1.7 Caselle di posta elettronica.....	14
1.8 Sistema di classificazione dei documenti.....	14
2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO.....	16
3. PIANO DI SICUREZZA.....	17
3.1 Generalità e obiettivi.....	17
3.2 Politiche generali della sicurezza adottate	18
3.3 Gestione dei documenti informatici.....	19
3.3.1 Componente organizzativa della sicurezza	20
3.3.2 Componente fisica della sicurezza	20
3.3.3 Componente logica della sicurezza	21
3.3.4 Componente infrastrutturale della sicurezza	22
3.3.5 Gestione delle registrazioni di sicurezza	23
3.3.6 Trasmissione e interscambio dei documenti informatici.....	24
3.4 Accesso ai documenti informatici.....	25
3.4.1 Utenti interni alla AOO	25
3.4.2 Utenti esterni alla AOO – Altre AOO/Amministrazioni	26
3.4.3 Utenti esterni alla AOO – Privati.....	26
3.5 Diritto di accesso e tutela dei dati personali.....	26
4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DEI DOCUMENTI INFORMATICI.....	28
4.1 Oggetti documentali gestiti	28
4.1.1 Documento informatico.....	28
4.1.2 Documento analogico.....	29
4.1.3 Documento ricevuto	29
4.1.4 Documento inviato.....	29

4.1.5	Documento interno formale e informale.....	30
4.1.6	Fascicolo documentale	31
4.2	Formazione dei documenti informatici	31
4.3	Sottoscrizione di documenti informatici.....	32
4.4	Uso della posta elettronica certificata.....	32
5.	DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI	34
5.1	Flusso dei documenti in ingresso alla AOO.....	36
5.1.1	Ricezione e accettazione	37
5.1.1.1	Ricezione dei documenti informatici.....	37
5.1.1.2	Ricezione di documenti cartacei a mezzo posta convenzionale.....	39
5.1.1.3	Errata ricezione di documenti analogici.....	39
5.1.1.4	Errata ricezione di documenti digitali	40
5.1.1.5	Rilascio di ricevute attestanti la ricezione di documenti informatici.....	40
5.1.1.6	Rilascio di ricevute attestanti la ricezione di documenti cartacei	40
5.1.1.7	Ricezione e trasmissione di documenti cartacei a mezzo fax.....	40
5.1.2	Registrazione di protocollo e classificazione.....	41
5.1.3	Assegnazione e smistamento interno	42
5.1.4	Fascicolazione.....	42
5.2	Flusso dei documenti inviati dalla AOO	43
5.2.1	Formazione e classificazione	44
5.2.2	Scansione dei documenti	44
5.2.3	Registrazione di protocollo e segnatrice.....	44
5.2.4	Trasmissione di documenti informatici.....	45
5.2.5	Trasmissione di documenti cartacei a mezzo posta.....	46
5.2.6	Fascicolazione.....	47
5.3	Matrice della responsabilità	47
6.	REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI RICEVUTI (IN ENTRATA).....	49
6.1	Regole generali.....	49
6.2	Assegnazione e smistamento di documenti ricevuti in formato digitale.....	50
6.3	Assegnazione e smistamento di documenti ricevuti in formato cartaceo	51
6.4	Modifica delle assegnazioni.....	51
7.	UO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI.....	53
8.	ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	54

8.1	Documenti esclusi	54
8.2	Documenti soggetti a registrazione particolare.....	54
9.	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE	55
9.1	Misure di protezione e conservazione degli archivi pubblici.....	55
9.2	Sistema di classificazione dei documenti.....	55
9.3	Sistema di fascicolazione dei documenti.....	57
9.4	Archivio analogico dell'ANAC.....	58
9.4.1	Versamento dei fascicoli nell'archivio di deposito.....	58
9.4.2	Consultazione e movimentazione dell'archivio corrente, di deposito e storico.....	60
9.4.2.1	Consultazione da parte di personale interno ad ANAC	60
9.4.2.2	Consultazione da parte di personale esterno all'Amministrazione.....	61
9.4.3	Scarto dei documenti.....	62
10.	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.....	63
10.1	Unicità del protocollo informatico.....	63
10.2	Registro giornaliero di protocollo.....	64
10.3	Registrazione di protocollo dei documenti.....	64
10.4	Segnatura di protocollo dei documenti	65
10.5	Annullamento delle registrazioni di protocollo.....	66
10.6	Livello di riservatezza	67
10.7	Casi particolari di registrazioni di protocollo.....	67
10.7.1	Corrispondenza riservata.....	67
10.7.2	Documenti indirizzati nominalmente al personale dell'ANAC.....	68
10.7.3	Corrispondenza di particolare rilevanza.....	69
10.7.4	Corrispondenza relativa a gare d'appalto o concorsi.....	69
10.7.5	Documentazione acquisita attraverso specifici sistemi ANAC	70
10.7.6	Documenti anonimi o non firmati	70
10.7.7	Documenti con più destinatari.....	70
10.7.8	Protocollazione di un numero consistente di documenti.....	71
10.7.9	Protocolli urgenti	71
10.7.10	Integrazioni documentarie.....	71
10.7.11	Messaggi di Posta Elettronica Ordinaria	72
11.	DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO	73
12.	MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA.....	74
13.	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI	75

13.1	Modalità di approvazione e aggiornamento del manuale	75
13.2	Pubblicità del presente Manuale.....	75
ALLEGATI	76

DATI DEL DOCUMENTO

Dati generali

Azione	Data	Nominativo	Funzione
Redazione	20/10/2023	Dott. Vincenzo Bonetti	Responsabile della Gestione Documentale
Revisione e consolidamento	20/10/2025	Dott. Vincenzo Bonetti	Responsabile della Gestione Documentale
Approvazione	10/12/2025	Consiglio ANAC	Consiglio ANAC

Registro delle versioni

Versione	Data emissione	Modifiche apportate	Descrizione delle modifiche
1.0	20/10/2023	Prima versione	Documento redatto in ottemperanza a quanto previsto dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate dall'AgID il 10 settembre 2020 (aggiornamento maggio 2021)
1.1	20/06/2024	Prima versione aggiornata	Integrazione del documento con la descrizione di talune modalità operative adottate nell'ambito della gestione del processo
1.2	20/10/2025	Prima versione consolidata	Consolidamento del documento

Acronimi e definizioni

Termine/Acronimo	Descrizione
AD	Active Directory
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea quale insieme di funzioni e strutture che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'art. 50, co. 4, del TUDA
ANAC	Autorità Nazionale Anticorruzione
Autorità	Si riferisce all'ANAC

Termine/Acronimo	Descrizione
CAdES	CMS Advanced Electronic Signatures. Tipo di firma digitale il cui contenuto è visualizzabile solo attraverso idonei software in grado di estrarre il documento sottoscritto dalla busta di firma
DGA	Direzione Generale degli Archivi
IDS	Intrusion Detection System
IPA	Indice delle Pubbliche Amministrazioni
IPS	Intrusion Prevention System
HTTPS	HyperText Transfer Protocol Secure
Massimario di Scarto	Piano di Conservazione
MdGD	Manuale della Gestione Documentale
PAdES	PDF Advanced Electronic Signatures. Tipo di firma digitale che può essere apposta esclusivamente su file PDF
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RC	Responsabile della Conservazione
RGD	Responsabile della Gestione Documentale
RPA	Responsabile del Procedimento Amministrativo - il Dirigente e/o il Funzionario che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi a una specifica questione
SdP	Il Sistema di Protocollo informatico adottato da ANAC per implementare il servizio di protocollo informatico
SGD	Sistema di gestione documentale
SMTP	Simple Mail Transfer Protocol
Titolario	Piano di Classificazione
UO	Unità Organizzative - Uffici Dirigenziali in cui si articola l'AOO

Riferimenti

Codice riferimento	Codice	Descrizione
RIF.001	Linee guida sulla formazione, gestione e conservazione dei documenti informatici	Con la determinazione n. 371/2021 l'AgID ha adottato l'attuale versione delle "Linee guida sulla formazione, gestione e conservazione dei documenti informatici", entrata in vigore il 1° gennaio 2022. (https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico.pdf)
RIF.002	Piano Sicurezza e Privacy	Piano per la sicurezza delle informazioni e la tutela dei dati personali dell'Autorità Nazionale Anticorruzione.
RIF.003	Procedure Operative Protocollo	Procedure operative interne per la gestione del protocollo informatico e dei flussi documentali dell'Autorità a supporto dell'operatività del personale ANAC.
RIF.004	Comunicato del Presidente ANAC del 27 aprile 2017 e ss.mm.ii.	Ambito d'intervento dell'Autorità Nazionale Anticorruzione

1. PRINCIPI GENERALI ED ORGANIZZATIVI

1.1 Premesse

Il presente Manuale della Gestione Documentale (MdGD, nel seguito anche *Manuale*) è stato redatto in applicazione della normativa vigente in ambito di formazione, gestione e conservazione dei documenti, in ottemperanza alle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* [RIF.001].

Obiettivo del presente MdGD è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che, a diverso titolo, interagiscono con l'Amministrazione.

Il *Manuale* è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti ANAC e ai soggetti esterni che si relazionano con l'Amministrazione.

1.2 Ambito di applicazione del manuale

In coerenza con il quadro normativo di riferimento il MdGD è volto a disciplinare le attività di formazione, registrazione, classificazione, fascicolazione dei documenti sia cartacei sia digitali dell'Autorità Nazionale Anticorruzione" di seguito denominata" ANAC, Autorità o anche Amministrazione. Tali attività sono finalizzate ad assicurare l'identificazione e la reperibilità dei documenti amministrativi formati o acquisiti dall'Autorità nell'ambito dell'esercizio delle proprie attività istituzionali. Inoltre, la registrazione di protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

In tale ottica, il protocollo informatico assume un ruolo strategico e realizza le condizioni operative per una efficace ed efficiente gestione del flusso informativo e documentale interno, anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa, configurandosi come lo strumento per attuare concretamente i principi previsti dalla Legge 241/1990 sul procedimento amministrativo.

Il Manuale disciplina in particolare:

- ✓ la ricezione da parte del Servizio di Protocollo della documentazione in entrata, la successiva assegnazione agli uffici competenti e al Responsabile del Procedimento Amministrativo (RPA), ovvero il soggetto responsabile della lavorazione della pratica amministrativa;
- ✓ la gestione della corrispondenza in uscita dagli uffici dell'Autorità;
- ✓ la classificazione dei documenti sulla base di un Piano di Classificazione e Conservazione, volta ad assicurare una stratificazione ordinata dell'archivio e alla sua corretta conservazione;
- ✓ la formazione dei fascicoli, prodromica ad una corretta ed efficiente gestione archivistica.

1.3 Riferimenti normativi

Ai fini del presente Manuale si intende per:

Legge sul procedimento amministrativo: la Legge 7 agosto 1990, n. 241 - Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Testo Unico Documentazione Amministrativa o TUDA: il Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 e s.m.i. - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Regolamento Commissioni di sorveglianza: il Decreto del Presidente della Repubblica 37/2001 - Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato.

Codice per la protezione dei dati personali: il Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. - Codice in materia di protezione dei dati personali.

Codice dei Beni Culturali: il Decreto Legislativo 42/2004 e s.m.i. - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.

Codice Amministrazione Digitale o CAD: il Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'Amministrazione Digitale.

Decreto Trasparenza: il Decreto Legislativo 14 marzo 2013, n. 33 - Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle pubbliche amministrazioni.

Regole tecniche per il protocollo informatico: il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82", parzialmente abrogato dalle Linee Guida AgID, in riferimento a: art. 2 comma 1, Oggetto e ambito di applicazione; art. 6, Funzionalità; art. 9, Formato della segnatura di protocollo; art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; art. 20, Segnatura di protocollo dei documenti trasmessi; art. 21, Informazioni da includere nella segnatura.

Regole tecniche in materia di firme elettroniche: il Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

Regolamento eIDAS (electronic IDentification Authentication and Signature): Regolamento UE n° 910/2014 sull'identità digitale che ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

GDPR (General Data Protection Regulation): il Regolamento del Parlamento europeo e del Consiglio, del 27 aprile 2016, n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati Legge 7 agosto 1990, n. 241 e successive modifiche e integrazioni "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi".

Linee Guida IPA: le Linee guida AgID dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

Linee guida sulla formazione, gestione e conservazione dei documenti informatici: le Linee guida adottate dall'AgID a decorrere da 1° gennaio 2022 sulla formazione, gestione e conservazione dei documenti informatici.

Regolamento Accesso agli Atti: Regolamento disciplinante i procedimenti relativi all'accesso civico, all'accesso civico generalizzato ai dati e ai documenti detenuti dall' ANAC e all'accesso ai documenti amministrativi ai sensi della legge 241/1990 di cui alla delibera n. 1019 del 24.10.2018 e s.m.i.

1.4 Caratterizzazione dell'Area Organizzativa Omogenea

Per la gestione dei documenti, è stata individuata un'unica Area Organizzativa Omogenea (AOO), denominata "ANAC", che è composta dall'insieme di tutte le Unità Organizzative (UO) individuate nell'atto di organizzazione delle aree e degli uffici dell'Amministrazione.

Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, denominato anche Servizio di Protocollo e Gestione Documentale (SGD) o semplicemente Servizio di protocollo, e all'interno della AOO il sistema di protocollazione è unico.

1.5 Modello organizzativo del Servizio di Protocollo

Il Servizio di Protocollo dell'Autorità è centralizzato per la corrispondenza in entrata, mentre è decentralizzato per la corrispondenza in uscita.

Nello specifico, il SGD svolge i compiti di UO di registrazione di protocollo principale dell'ANAC per la corrispondenza in entrata, demandando la protocollazione e classificazione della corrispondenza in uscita alla UO competente per materia del documento.

La scelta di un modello decentrato - riguardo alla protocollazione in uscita - risiede nell'esigenza di attribuire autonomia agli Uffici, anche in ragione della numerosità degli atti prodotti dal personale dell'ANAC nell'ambito delle proprie competenze e trasmessi a soggetti esterni.

Il SGD è coordinato dal Dirigente competente posto che la responsabilità dello stesso rimane in capo al Responsabile della Gestione Documentale (di seguito RGD), affiancato dal Responsabile della Conservazione (di seguito RC).

1.6 Servizio per la gestione informatica del protocollo

Ai sensi dell'art. 61, co. 3, del TUDA, nell'ambito del Servizio di Protocollo sono assicurate le seguenti funzioni:

- ✓ abilitazione del personale dell'ANAC all'utilizzo del protocollo informatico definendo per ciascuno di essi il tipo di funzioni a disposizione;
- ✓ garanzia del rispetto delle disposizioni durante le operazioni di registrazione e di segnatura di protocollo;
- ✓ garanzia della corretta produzione e conservazione del registro giornaliero di protocollo;
- ✓ cura delle funzionalità del sistema di protocollo informatico di comune accordo con i servizi di gestione dei sistemi informativi affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- ✓ conservazione delle copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza attraverso i servizi di gestione dei sistemi informativi in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- ✓ garanzia del buon funzionamento degli strumenti e del rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
- ✓ autorizzazione - con provvedimenti *ad hoc* - delle operazioni di annullamento della registrazione di protocollo (art. 54 del D.P.R. n. 445/2000);
- ✓ vigila sull'osservanza delle disposizioni del TUDA da parte del personale autorizzato e degli incaricati.

Nell'ambito del SGD i compiti del RGD e del RC, come pure i contenuti del presente Manuale, sono disciplinati nelle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*.

1.7 Caselle di posta elettronica

L'ANAC ha istituito una casella istituzionale di Posta Elettronica Certificata (PEC) (protocollo@pec.anticorruzione.it) per la ricezione e l'invio della corrispondenza dell'Autorità. La casella è pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA) ed è accessibile - per la ricezione di documenti - solo all'UO preposta all'erogazione del Servizio di Protocollo, mentre per la manutenzione e la gestione tecnica è accessibile agli uffici informatici dell'ANAC. La casella PEC istituzionale è configurata per accettare anche la ricezione di messaggi di posta elettronica ordinaria (PEO) soggetti anch'essi a protocollazione, alla stregua di un messaggio pervenuto attraverso PEC.

Il personale del Servizio di Protocollo presidia, inoltre, la casella PEC accessofoia@pec.anticorruzione.it utilizzata per la ricezione delle istanze di accesso civico generalizzato.

Sull'indice IPA è altresì presente la casella fatture@pec.anticorruzione.it utilizzata dall'ufficio preposta alla ricezione delle fatture passive.

Come per la casella PEC istituzionale, gli uffici informatici dell'ANAC si occupano della sola manutenzione e gestione tecnica delle stesse caselle.

Ogni ufficio è dotato di mail istituzionale non certificata; le mail sono riportate nel sito istituzionale secondo quanto stabilito dal *Decreto Trasparenza*.

1.8 Sistema di classificazione dei documenti

L'ANAC ha adottato un Titolario o Piano di classificazione. Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione

funzionale dell'AOO. Esso consente di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi. Il Piano di classificazione è dettagliatamente illustrato nel successivo capitolo 9, *Sistema di classificazione, fascicolazione e conservazione*.

2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO

Tutti i documenti protocollati sono registrati nel registro ufficiale di protocollo informatico. Pertanto, tutti gli eventuali registri di protocollo, interni alle UO, diversi dal registro ufficiale di protocollo informatico, sono aboliti ed eliminati.

3. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, in relazione alle norme sulla protezione dei dati personali e alle Misure Minime di sicurezza ICT definite da AgID, così come previsto dalle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*.

Tali misure sono state predisposte dall'RGD nel rispetto delle misure minime di sicurezza previste nel *Codice in materia di protezione dei dati personali*, d'intesa con il RC e il Responsabile dei sistemi informativi.

3.1 Generalità e obiettivi

Le misure per la sicurezza informatica garantiscono che i documenti e le informazioni in possesso dell'ANAC siano disponibili, integre e riservate e che i dati personali, sensibili e/o giudiziari vengano conservati, mediante l'adozione di adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o di perdita anche fortuita, nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Tali misure hanno anche l'obiettivo di garantire che l'organizzazione sia conforme alle normative e alle politiche interne ed esterne in materia di sicurezza informatica, oltreché di sensibilizzare gli utenti dell'Amministrazione sulla loro importanza e sui rischi associati ad un uso improprio dei sistemi e delle informazioni.

Le misure descritte si basano sul risultato di un *assessment* relativo alla verifica della sicurezza dei dati e dei documenti trattati svolto al fine di mantenere la sicurezza informatica dell'organizzazione e mitigare i rischi associati alle minacce informatiche.

Le misure definiscono:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'A00;
- le modalità di gestione dei documenti informatici con particolare riferimento agli aspetti operativi della sicurezza in relazione alle Misure minime di sicurezza, di cui al Disciplinare tecnico richiamato nell'allegato B) relativo al *Codice in materia di protezione dei dati personali*;
- le modalità di accesso ai documenti informatici.

Le misure di sicurezza sono da considerarsi come parti integranti del Piano di Sicurezza generale ANAC [RIF.002] e ad esso si fa riferimento per una loro descrizione di dettaglio.

3.2 Politiche generali della sicurezza adottate

Il RGD, al fine di assicurare la sicurezza dell'impianto tecnologico dell'A00, la riservatezza delle informazioni registrate nelle banche dati e l'univoca identificazione degli utenti interni ed esterni, assicura le seguenti misure tecniche e organizzative:

- protezione periferica della Intranet dell'A00;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del Sistema di Protocollo (SdP), di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione (vedi anche il paragrafo 3.4 *Accesso ai documenti informatici*);
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e dell'applicativo contenenti le informazioni;
- conservazione, a cura del RGD, delle copie di riserva (Backup) dei dati e dei documenti, in locali diversi e lontani dai locali in cui è installato il sistema di elaborazione di esercizio che ospita il SdP;
- Disaster Recovery al fine di ripristinare le funzionalità e la disponibilità del sistema.

3.3 Gestione dei documenti informatici

Il SdP:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti interni, in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Inoltre, il sistema informatico è configurato in maniera tale da consentire:

- la sicurezza dei documenti contenuti nel sistema di gestione documentale con l'accesso al server del SdP limitato ai soli utenti autorizzati, impedendo qualsiasi accesso non autorizzato dall'esterno;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificabilità. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il SdP utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto, dalle Autorità competenti;
- l'accesso ai documenti memorizzati nel SdP solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto, dalle forze dell'ordine.

3.3.1 Componente organizzativa della sicurezza

Nella conduzione del sistema informativo dell'ANAC, l'organizzazione per la componente sicurezza prevede la classificazione dei dati in base alla loro importanza e al livello di rischio associato, il controllo degli accessi, il backup e ripristino dei dati e la conformità alle normative esterne ed interne in materia di sicurezza informatica.

Di seguito sono specificate le misure adottate:

- presenza di una procedura relativa al controllo degli accessi;
- presenza di una procedura di rilascio delle abilitazioni di accesso al SdP;
- accesso, uso e gestione dei dati sensibili in linea con il GDPR;
- presenza di una procedura di backup management;
- policy di password management;
- presenza di firewall;
- formazione e consapevolezza degli utenti;
- monitoraggio e reporting di monitoraggio dei log di sicurezza, nonché generazione di report sulle attività sospette.

3.3.2 Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- autorizzazione preventiva per l'accesso;
- accesso controllato da serratura con tracciatura;
- registro di prelevamento della chiave per accedere al locale in cui è presente il server.

Le misure di sicurezza prevedono un'adeguata protezione fisica dei locali e delle apparecchiature attraverso un'architettura multilivello:

- a livello di sede dell'AOO che ospita il sistema informatico:

- è stabilita un'adeguata protezione fisica delle strutture da calamità naturali, attacchi malevoli o accidentali (ad es. incendio, inondazione, terremoto, esplosione, disordini civili e altre forme di disastri naturali o provocati dall'uomo);
- vengono protette le apparecchiature da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari (ad esempio: approvvigionamento idrico, gas, fognature, ventilazione e aria condizionata, etc);
- a livello di locale che ospita il nastro contenente le copie di backup:
 - è garantita la possibilità di accedere alla cassaforte solo da parte del RGD e da coloro che sono preventivamente autorizzati.

3.3.3 Componente logica della sicurezza

La componente logica della sicurezza si riferisce alla progettazione, implementazione e gestione di controlli logici che garantiscono la sicurezza dei dati, delle informazioni e dei messaggi. Questi controlli logici sono finalizzati a garantire la protezione dei dati da accessi non autorizzati, alterazioni, distruzioni o divulgazioni non autorizzate.

In particolare, la componente logica della sicurezza si occupa di garantire la conformità dei sistemi informatici ai requisiti di sicurezza, tra cui l'integrità, la riservatezza, la disponibilità e il non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del SdP, è stata realizzata attraverso:

- accesso controllato (l'accesso al sistema e ai dati è limitato solo agli utenti autorizzati);
- utilizzo di firewall per garantire la sicurezza del software;
- monitoraggio dei log di sicurezza anche attraverso sistemi di allarme in caso si verifichi un accesso anomalo;
- protezione dei dati sensibili presenti all'interno del sistema informativo da accessi non autorizzati e possibili attacchi informatici attraverso la gestione del backup, la classificazione dei dati e la visibilità solo agli utenti autorizzati;

- sicurezza delle reti.

Il SdP adottato:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

3.3.4 Componente infrastrutturale della sicurezza

La componente infrastrutturale della sicurezza si riferisce all'insieme di hardware, software e reti che supportano la gestione e il controllo delle informazioni all'interno di un'organizzazione. L'obiettivo principale della componente infrastrutturale è garantire la disponibilità, l'integrità, la riservatezza e la non ripudiabilità dei dati e delle informazioni.

Per implementare la componente infrastrutturale della sicurezza, sono state adottate le seguenti misure:

- sistemi antiintrusione di tipo IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) affinché le reti siano gestite in modo tale da proteggere le informazioni dell'applicazione;
- specifici requisiti di configurazione/connessione alle reti wireless per ogni tipologia di accesso da remoto, guide operative e restrizioni al solo personale autorizzato all'accesso in accordo con quanto previsto dalle politiche interne adottate dall'Amministrazione;
- modelli di Hardening standard che definiscono specifiche configurazioni del SdP che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità dello stesso, migliorandone pertanto la sicurezza complessiva;
- utilizzo del protocollo sicuro HTTPS che garantisce la protezione delle informazioni attraverso un sistema di tipo client-server.

3.3.5 Gestione delle registrazioni di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo presenti o transitate sul SdP che è opportuno mantenere per verificare la conformità alle politiche di sicurezza, per risolvere problemi tecnici, per monitorare le attività degli utenti, per rilevare eventuali attacchi informatici e poiché possono essere necessarie in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso.

Nello specifico, le registrazioni di sicurezza sono costituite da:

- log di sistema generati dal sistema operativo;
- log dei dispositivi di protezione periferica del sistema informatico (IDS, sensori di rete e firewall);
- registrazioni effettuate dallo stesso SdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- raccolta dei log di sicurezza da tutti i dispositivi e le applicazioni all'interno del sistema informativo attraverso uno strumento di archiviazione esterna accessibile solo ad alcuni utenti autorizzati. Il sistema garantisce che siano tracciate tutte le informazioni chiave relative a ogni evento, come la data, l'ora e la tipologia di operazione effettuata;
- accesso ai log solo da parte dell'amministratore di sistema;
- analisi dei log di sicurezza periodica per identificare eventuali attività sospette o anomale;
- conservazione dei log di sicurezza per un periodo di tempo adeguato a consentire la successiva analisi e la ricerca di eventuali attività sospette o anomale;
- protezione dei log di sicurezza da accessi e modifiche non autorizzati;
- notifiche di sicurezza immediate nei confronti del personale preposto in caso di attività sospette o anomale identificate nei log di sicurezza tramite sistemi di allarme;
- audit dei log di sicurezza con revisione regolare per garantire che i requisiti di sicurezza siano stati soddisfatti e per identificare eventuali aree di miglioramento.

3.3.6 Trasmissione e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

I dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre Pubbliche Amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale ANAC, oltre alle funzioni di un server Simple Mail Transfer Protocol (SMTP) tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto *Codice per la protezione dei dati personali*.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle Amministrazioni coinvolte nello scambio dei messaggi.

3.4 Accesso ai documenti informatici

3.4.1 Utenti interni alla AOO

La sicurezza delle registrazioni di protocollo e dei documenti è garantita da un sistema di autenticazione centralizzato che gestisce abilitazione ed autenticazione degli utenti interni all'ANAC. La gestione e la titolarità delle credenziali è affidata al sistema di Active Directory (AD) e gli utenti sono automaticamente autenticati per l'accesso al SdP attraverso un'integrazione con tale sistema.

All'interno del SdP, gli utenti hanno autorizzazioni di accesso differenziate in base alle rispettive competenze. Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente:
 - pubblica che permette l'identificazione dell'utente da parte del sistema (username);
 - privata o riservata di autenticazione (password);
- un'autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene;
- una visibilità sui documenti che può riguardare:
 - tutti i protocolli della UO;
 - tutti i protocolli del RPA;
 - solo i protocolli inseriti dall'utente medesimo;
 - tutti i protocolli, compresi i riservati sulla base della competenza.

Ciascun utente del SdP può accedere solamente ai documenti che sono stati assegnati alla sua UO o ad una UO ad essa subordinata.

Il sistema consente altresì di associare un livello di riservatezza per ogni tipo di documento trattato dall'Amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio. Nel caso in cui sia effettuata una protocollazione riservata, la visibilità completa del documento è possibile solo all'utente

“amministratore”, all’utente assegnatario del documento e all’operatore di protocollo che ha effettuato la registrazione.

Lo username, essendo attribuito ad uno specifico utente, permette di risalire alle operazioni compiute sul SdP dall’utente. Il SdP memorizza tutte le operazioni eseguite dagli utenti registrando data, ora e operazione eseguita. In particolare, il SdP memorizza le operazioni subite da un documento relative alle attività di registrazione di protocollo, classificazione e fascicolazione.

Al fine di garantire la sicurezza del sistema, nonché la riservatezza delle informazioni registrate, la password deve essere modificata con cadenza almeno trimestrale e, in nessun caso, va comunicata ad altri utenti.

Sulla base di provvedimenti formali di assegnazione del personale alle UO, i diversi livelli di autorizzazione sono assegnati agli utenti dal RGD, che si avvale di un profilo da amministratore per l’abilitazione di un utente nel SdP.

3.4.2 Utenti esterni alla AOO – Altre AOO/Amministrazioni

Non sono disponibili funzioni per l’accesso, per via telematica, ai documenti da parte di utenti esterni appartenenti ad altre Amministrazioni.

3.4.3 Utenti esterni alla AOO – Privati

Non sono disponibili funzioni per l’esercizio diretto, per via telematica, del diritto di accesso ai documenti da parte di utenti privati.

3.5 Diritto di accesso e tutela dei dati personali

La gestione dei procedimenti amministrativi, unitamente alla gestione dei documenti e del protocollo informatico, sono ispirati al rispetto delle norme in materia di diritto di accesso e di

protezione dei dati personali e sensibili di cui al *Codice in materia di protezione dei dati personali* e al *GDPR*, soprattutto con particolare riferimento al concetto di accountability ed alla capacità di adottare un processo efficace per la protezione degli stessi in grado di ridurre al minimo i rischi di una loro possibile violazione.

L'ANAC disciplina il diritto di accesso e la consultazione per fini amministrativi da parte di terzi dei documenti amministrativi e dei fascicoli formati o detenuti stabilmente dall'Autorità, in conformità alla normativa vigente. Valgono in tal senso le disposizioni contenute nel *Regolamento Accesso agli Atti*. Il documento è pubblicato sul sito web dell'ANAC e contiene tutte le indicazioni necessarie per esercitare le diverse tipologie di accesso agli atti.

L'ANAC disciplina le modalità di accesso civico e di accesso civico generalizzato ai dati e documenti detenuti attraverso il succitato Regolamento.

L'ANAC, quale Amministrazione a cui sono riconducibili i dati di protocollo e quelli personali contenuti nella documentazione amministrativa di propria competenza, dà attuazione alle disposizioni contenute nel *Codice in materia di protezione dei dati personali* con atti aventi rilevanza interna ed esterna e nel *GDPR*.

Alla luce di quanto sopra, il personale preposto all'apertura e alla registrazione della corrispondenza è regolarmente autorizzato al trattamento dei dati personali.

Invero, il personale tutto nell'esercizio delle proprie funzioni e nel rispetto di quanto disciplinato nel Codice di comportamento ANAC, è tenuto all'osservanza del segreto d'ufficio, nonché dei doveri e degli obblighi previsti dalla normativa di riferimento, a non trarre benefici personali o a nuocere a terzi e all'immagine dell'ANAC dalla conoscenza di particolari circostanze desumibili dai documenti.

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DEI DOCUMENTI INFORMATICI

4.1 Oggetti documentali gestiti

Nell'ambito del processo di gestione documentale, il documento amministrativo è così classificabile:

- in termini tecnologici del supporto di rappresentazione dell'originale:
 - informatico;
 - analogico;
- in termini operativi:
 - ricevuto (o anche in entrata);
 - inviato (o anche in uscita);
 - interno formale e informale.

Ogni documento ha significato in quanto parte di un contesto più ampio costituito da ciò che precede e da ciò che segue. Il documento, in quanto elemento prodotto o riferito ad un'attività amministrativa, è inserito in un insieme di documenti relativi ad una medesima attività o materia nella forma di fascicolo o aggregazione documentale.

4.1.1 Documento informatico

Per documento informatico si intende il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. p, del CAD). L'ANAC forma gli originali dei propri documenti con mezzi informatici secondo le disposizioni contenute nel CAD e le regole tecniche di cui all'art. 71 dello stesso (*Linee guida sulla formazione, gestione e conservazione dei documenti informatici*). Qualsiasi documento deve riportare un solo protocollo e può fare riferimento a più aggregati documentali (fascicoli). Le firme necessarie alla redazione

e perfezione giuridica del documento in uscita o interno devono essere apposte prima della sua protocollazione.

4.1.2 Documento analogico

A norma dell'art. 1 lettera p-bis) del CAD per documento analogico si intende la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti. Il documento analogico è prodotto con strumenti informatici di videoscrittura e, solo in casi eccezionali, con strumenti analogici. L'originale è cartaceo e dotato di firma autografa.

4.1.3 Documento ricevuto

I documenti ricevuti in ingresso sono tutti gli atti aventi rilevanza giuridico-probatoria prodotti da soggetti esterni ed acquisiti dall'ANAC nell'esercizio delle sue funzioni. I documenti informatici sono recapitati a mezzo posta elettronica certificata o convenzionale, su supporto rimovibile (quale, ad esempio, CD ROM, DVD, pen drive, etc) consegnato direttamente al personale del Servizio di Protocollo, attraverso fax server nel caso di comunicazioni provenienti da privati o ancora attraverso i servizi online. I documenti analogici trasmessi da soggetti esterni all'Amministrazione sono recapitati a mezzo posta convenzionale o corriere, a mezzo posta raccomandata, con consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata al Servizio di Protocollo.

4.1.4 Documento inviato

I documenti in uscita inviati sono tutti gli atti aventi rilevanza giuridico-probatoria prodotti dal personale dell'ANAC nell'esercizio delle proprie funzioni e trasmessi a soggetti esterni. I documenti informatici sono trasmessi ai destinatari per mezzo della posta elettronica certificata

o mediante e-mail istituzionali. In altri casi, il documento informatico può essere riversato su supporto rimovibile non modificabile ed inviato al destinatario. I documenti su supporto cartaceo sono inviati a mezzo servizi postali.

4.1.5 Documento interno formale e informale

I documenti interni sono tutti gli atti prodotti all'interno dell'ANAC, generalmente con tecnologie informatiche e possono essere:

- ✓ di natura prevalentemente informativa (documenti interni informali);
- ✓ di natura prevalentemente giuridico-probatoria (documenti interni formali).

I documenti interni di natura informativa quali: mere comunicazioni interne scambiate tra uffici, richieste di interventi di manutenzione pc, etc non vanno protocollati. Di regola, lo scambio di tali documenti avviene per mezzo della posta elettronica interna.

I documenti interni di natura prevalentemente giuridico-probatoria, ossia tutti gli atti redatti dal personale dell'ANAC nell'esercizio dell'espletamento delle proprie funzioni, volti a documentare le attività istruttorie di competenza, devono essere protocollati.

Pertanto, gli appunti e/o le relazioni istruttorie, pareri inviati al Consiglio, verbali di audizioni svolte presso gli Uffici vanno protocollati, selezionando la casella "interno" del SdP.

Nei casi in cui il documento interno sia di tipo analogico, lo scambio può avvenire con i mezzi tradizionali all'interno dell'Amministrazione: il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa e successivamente protocollato.

Non possono essere trattati come documenti interni quelli redatti da personale in servizio presso l'ANAC ed indirizzati agli Organi e/o agli Uffici della stessa Autorità (richieste, comunicazioni, note sindacali), infatti tali documenti devono essere protocollati come provenienti dall'esterno.

4.1.6 Fascicolo documentale

In termini archivistici il fascicolo è lo strumento che consente l'aggregazione dei documenti in base al procedimento o allo specifico "affare" e al suo interno i documenti sono archiviati secondo l'ordine cronologico di registrazione.

4.2 Formazione dei documenti informatici

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adotta preferibilmente il formato PDF.

Il documento informatico, identificato in modo univoco e persistente, è memorizzato nel SdP in uso nella AOO che ne garantisce l'inalterabilità, la riservatezza e la fruibilità da parte degli utenti dotati di adeguate autorizzazioni.

Per quanto riguarda i documenti informatici ricevuti sono accettati tutti i formati indicati come "idonei" dall'Allegato 2 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*. Nell'Allegato 1 al presente manuale si riporta un elenco di sintesi periodicamente aggiornato rispetto alle indicazioni delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*.

Al documento informatico imm modificabile vengono associati i metadati che sono stati generati durante la sua formazione coerentemente con quanto indicato dalle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*. Nell'Allegato 2 al presente manuale è riportata la scheda informativa dei principali metadati trattati per il documento e per il fascicolo informatico.

4.3 Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, al fine di garantirne l'immodificabilità, sono convertiti, ove possibile, nel formato Acrobat PDF o comunque in uno dei formati idonei riportati nell'Allegato 1. Si adotta preferibilmente il formato di firma PADES.

La sottoscrizione con firma digitale dei documenti informatici è utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti o qualsiasi altro "file" digitale con valenza giuridico-probatoria. La sottoscrizione con firma digitale soddisfa i requisiti di integrità e non ripudio del documento.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente.

4.4 Uso della posta elettronica certificata

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante l'uso della Posta elettronica Certificata. L'utilizzo della posta elettronica certificata (PEC) consente di:

- ✓ firmare elettronicamente il messaggio;
- ✓ conoscere in modo inequivocabile la data e l'ora di trasmissione;
- ✓ garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- ✓ interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema PEC. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno, che sono classificati in:

- ✓ conferma di ricezione;
- ✓ notifica di eccezione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Il documento informatico trasmesso per PEC si intende inviato, nonché pervenuto al destinatario se trasmesso all'indirizzo PEC da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente, sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale, nei casi consentiti dalla legge, alla notifica per mezzo della posta.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.




Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

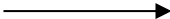
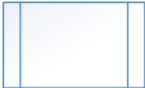
- ✓ ricevuti dalla AOO;
- ✓ inviati all'esterno della AOO;
- ✓ inviati in modo formale all'interno della AOO.

Le comunicazioni informali, intese come lo scambio di informazioni tra uffici, con o senza documenti allegati, delle quali è facoltativa la conservazione, sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo e i flussi di lavorazione dei documenti.

I flussi di lavorazione sono rappresentati graficamente sotto forma di flow-chart (diagramma di flusso) che evidenzia:

- ✓ le attività da svolgere;
- ✓ gli attori coinvolti;
- ✓ gli input e gli output previsti.

Simbolo	Denominazione	Descrizione
	Inizio/Fine	Rappresenta l'inizio/la fine di un processo
	Attività	Rappresenta un'attività del processo.
	Decisione	Rappresenta un momento decisionale nell'ambito del processo. A seconda dei possibili esiti del momento decisionale, da esso derivano due diversi percorsi alternativi.

Simbolo	Denominazione	Descrizione
	Linee di flusso	Connette le diverse attività secondo la sequenza con cui devono essere eseguite.
	Processo secondario	Fa riferimento ad un ulteriore processo, non oggetto di rappresentazione nello specifico flusso

Si rimanda al documento “Procedure Operative Protocollo” [RIF.003] per la descrizione di dettaglio delle regole e delle modalità di lavorazione dei documenti.

5.1 Flusso dei documenti in ingresso alla AOO

Si riporta il diagramma di flusso che sintetizza la gestione dei documenti ricevuti dalla AOO.

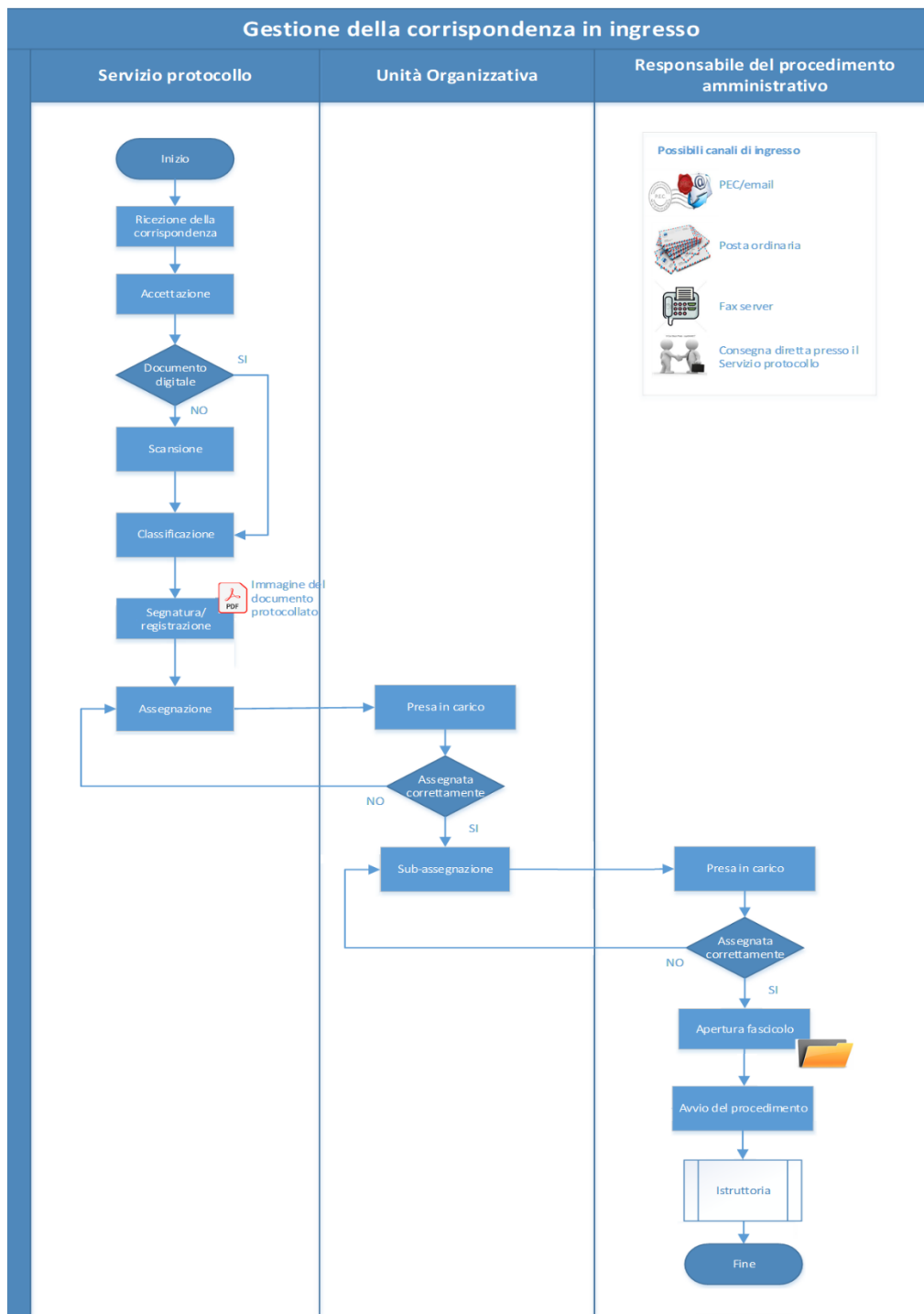


Figura 1 - Diagramma di flusso del processo di gestione dei documenti in ingresso

5.1.1 Ricezione e accettazione

5.1.1.1 Ricezione dei documenti informatici

Di norma la ricezione dei documenti informatici è assicurata tramite le caselle di PEC, quella istituzionale (protocollo@pec.anticorruzione.it) *in primis* e le caselle accessofoia@pec.anticorruzione.it e fatture@pec.anticorruzione.it, accessibili in ingresso rispettivamente, al personale addetto al Servizio di Protocollo e all'Ufficio preposto alla gestione delle fatture.

Per le "segnalazioni di vigilanza" il canale unico di accettazione è rappresentato dal modulo web disponibile sul sito istituzionale che consente al segnalante di inviare all'ANAC le segnalazioni in materia di vigilanza su contratti pubblici, trasparenza ed anticorruzione.

Le mail/PEC la cui tipologia documentale ed Ufficio destinatario sono individuabili automaticamente tramite mittente e/o parole chiave all'interno del campo "oggetto", in automatico sono registrate e protocollate in ingresso nonché assegnate direttamente all'Ufficio competente. Il personale del Servizio di Protocollo controlla quotidianamente messaggi pervenuti nella casella di posta istituzionale, non soggetti a protocollazione automatica e, previa verifica della bontà e dell'integrità del messaggio, nonché della reale competenza rispetto alle attività istituzionali secondo quanto previsto dal Comunicato del Presidente ANAC [RIF.004], procede alla registrazione di protocollo, di norma (a meno di particolari eccezioni descritte nel seguito), secondo l'ordine cronologico di arrivo.

Nel caso in cui il messaggio pervenuto sia illeggibile, incompleto o affetto da virus, il personale del Servizio di Protocollo deve segnalare la circostanza al mittente, indicando che lo stesso non verrà sottoposto a protocollazione. Analogamente, per i documenti ricevuti in un formato non conforme a uno dei formati "idonei" indicati nell'Allegato 1, il personale del Servizio di Protocollo deve segnalare la circostanza al mittente, indicando che lo stesso non verrà sottoposto a protocollazione e invitandolo ad inviare nuovamente il documento in un formato idoneo. In via

eccezionale e solo in caso di giustificata motivazione, sentito il RGD e il RC, il personale del Servizio di protocollo procede alla protocollazione del documento nel formato non idoneo.

I documenti informatici in arrivo possono essere dotati di firma elettronica (semplice o avanzata, qualificata o digitale) o non firmati.

Ai sensi dell'art. 20, co 1-bis, del CAD il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 del Codice Civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente requisiti tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.

In particolare, la firma elettronica utilizzata per inviare e ricevere documenti da e per l'ANAC e per sottoscrivere documenti, costituisce l'unico strumento che soddisfa i requisiti di sicurezza dell'identificabilità del sottoscrittore, nonché dell'integrità ed immodificabilità del documento.

Secondo quanto stabilito dall'art. 24 del CAD, l'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente (co. 2). Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso (co. 3). Proprio tale certificato qualificato deve permettere di rilevare, secondo le regole tecniche di cui all'art. 71 dello stesso CAD, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso (co.4). L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione, salvo che lo stato di sospensione sia stato annullato (co. 4-bis).

Qualora il messaggio di posta elettronica non provenga da una casella PEC, ovvero non sia munito di firma elettronica, viene comunque protocollato, smistato ed assegnato. Il RPA valuta discrezionalmente l'opportunità di utilizzare o meno il documento così pervenuto.

5.1.1.2 Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti analogici che pervengono quotidianamente a mezzo posta sono sottoposti dal personale addetto al Servizio di Protocollo ad una preliminare verifica in merito all'indirizzo ed al destinatario sugli stessi apposti.

I documenti ricevuti via fax, per ciò che concerne la registrazione di protocollo, sono trattati come un documento cartaceo.

La busta si allega al documento per la parte relativa ai timbri postali.

Dopo aver accuratamente separato i documenti esclusi dalla registrazione del protocollo di cui all'art. 53, co. 5, del TUDA (gazzette ufficiali, bollettini ufficiali e notiziari della pubblica amministrazione, note di ricezione delle circolari e altre disposizioni, materiali statistici, atti preparatori interni, giornali, riviste, newsletter, libri, materiali pubblicitari, inviti) il personale del Servizio di Protocollo sollecitamente provvede alla registrazione, segnatura e classificazione dei documenti.

I documenti vengono scannerizzati, con acquisizione del relativo file nel sistema, ed assegnati alla UO di competenza, individuata in base al modello delle competenze, così come definito dall'atto di organizzazione delle Aree e degli Uffici dell'ANAC.

5.1.1.3 Errata ricezione di documenti analogici

Qualora al Servizio di Protocollo pervengano erroneamente documenti indirizzati ad altri Enti, vanno restituiti senza procedere alla protocollazione. Nel caso in cui la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia alla struttura destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

5.1.1.4 Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta istituzionale dell'ANAC o sui canali presidiati - così come descritti nel paragrafo 1.8 "Caselle di posta elettronica" - messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, il personale del Servizio di Protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa AOO".

5.1.1.5 Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici mediante la casella di PEC, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di PEC stessa.

5.1.1.6 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Il personale addetto al Servizio di Protocollo può rilasciare ricevute per i documenti che sono consegnati a mano. La ricevuta può essere prodotta solo a seguito della protocollazione attraverso un'apposita funzionalità del SdP.

5.1.1.7 Ricezione e trasmissione di documenti cartacei a mezzo fax

L'utilizzo del fax è ammesso solo con riferimento alla ricezione di corrispondenza da parte di privati, dal momento che, sulla base di quanto stabilito dall'art. 47 del CAD le comunicazioni di documenti tra pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa.

5.1.2 Registrazione di protocollo e classificazione

Le registrazioni di protocollo dei documenti ricevuti sono effettuate di norma nell'arco della giornata lavorativa e comunque non oltre due giorni lavorativi dal ricevimento, salvo situazioni eccezionali.

Il personale del Servizio di Protocollo provvede, contestualmente alla protocollazione dei documenti ricevuti, a classificare il documento nelle modalità descritte al § "9.2 Sistema di classificazione dei documenti".

Nel caso di ricezione di documenti afferenti questioni già in trattazione da parte dell'Autorità, il personale del Servizio di Protocollo, nell'ottica della collaborazione tra Uffici e dell'ottimizzazione dei procedimenti, prima di procedere all'operazione di registrazione ha cura di evidenziare i legami esistenti tra i documenti sulla base delle informazioni reperibili dai documenti stessi, da banche dati interne disponibili in consultazione al personale del Servizio di Protocollo o dal SdP mediante l'utilizzo della specifica funzione "allacci".

Nel caso di eccezionale carico di lavoro, che non permette di evadere la corrispondenza ricevuta nei tempi sopra indicati 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), con motivato provvedimento del RGD è autorizzato l'uso del "protocollo differito".

In particolare, il "protocollo differito" consiste nell'adozione di un provvedimento con il 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 il RGD deve indicare puntualmente nel provvedimento.

5.1.3 Assegnazione e smistamento interno

Il personale del SGD procede con la prima assegnazione/smistamento del documento ricevuto alla UO competente, che a sua volta procede con l'assegnazione al RPA nelle modalità indicate al cap. 6 "Regole di assegnazione e smistamento dei documenti ricevuti (in entrata)".

5.1.4 Fascicolazione

A seguito dell'assegnazione e relativa presa in carico, il RPA competente procede con l'apertura del fascicolo e/o con la fascicolazione del documento ricevuto, nella modalità indicate al § "9.3 Sistema di fascicolazione dei documenti".

5.2 Flusso dei documenti inviati dalla AOO

Si riporta il diagramma di flusso che sintetizza la gestione dei documenti:

- inviati all'esterno della AOO;
- inviati in modo formale all'interno della AOO.

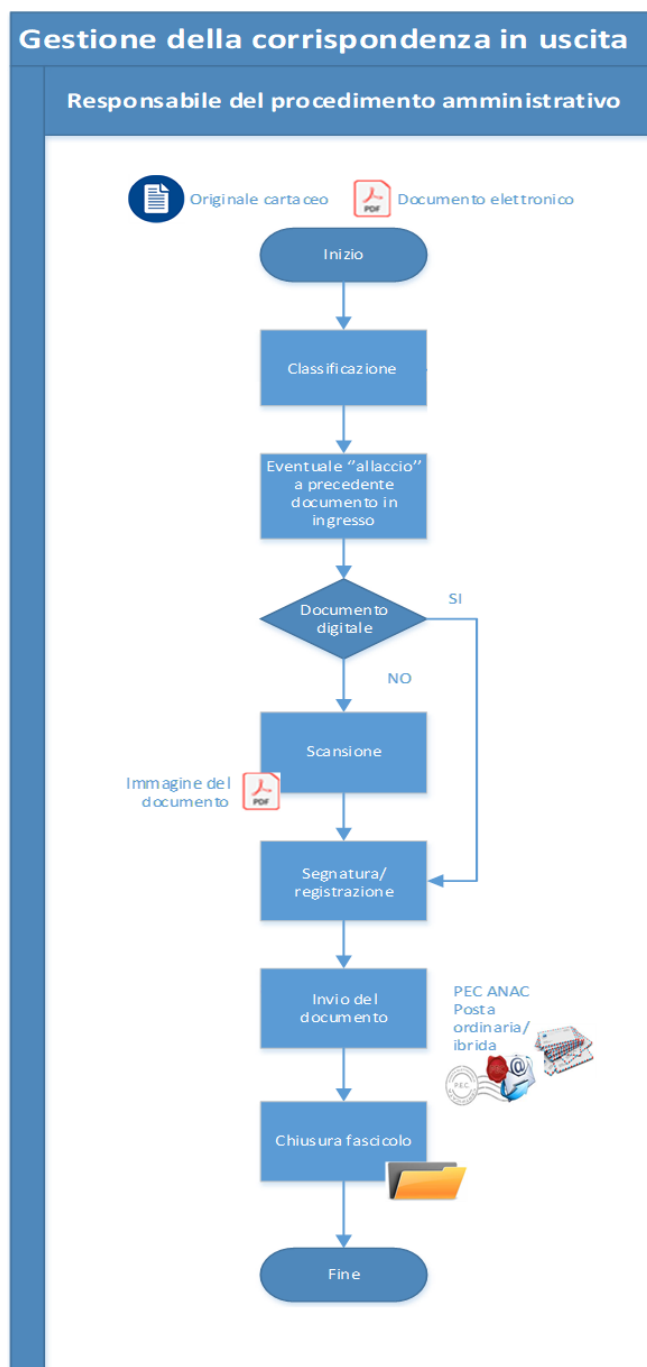


Figura 2 - Diagramma di flusso del processo di gestione dei documenti in uscita

5.2.1 Formazione e classificazione

L'UO mittente interna all'A00 produce, tramite il RPA, il documento in uscita nelle forme e nelle modalità più opportune sulla base di quanto indicato al cap. 4 "Modalità di utilizzo di strumenti informatici per la formazione e lo scambio dei documenti informatici".

I documenti sono classificati secondo il Titolario di classificazione: il RPA procede alla classificazione del documento in uscita nelle modalità descritte al § "9.2 Sistema di classificazione dei documenti".

5.2.2 Scansione dei documenti

I documenti in partenza nativi analogici sono scansionati e inseriti nel SdP nel formato PDF.

5.2.3 Registrazione di protocollo e segnatuta

Ogni UO è autorizzata dall'A00 per il tramite del RPA, a svolgere attività di registrazione di protocollo e apposizione della segnatuta per la corrispondenza in uscita. Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli RPA.

Gli RPA provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa. Se la verifica dà esito positivo, il documento viene protocollato e registrato nel registro di protocollo generale.

La protocollazione e la segnatuta della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UO abilitati in quanto collegati al SdP della A00 a cui appartengono.

Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatuta della missiva da inviare sono effettuate dal RPA.

In particolare, al momento della protocollazione degli atti in uscita vanno inserite nel SdP tutte quelle informazioni (allaccio, annotazioni, etc) ritenute necessarie per favorire una agevole ricerca degli atti, nonché un eventuale successivo monitoraggio delle pratiche stesse.

Ciascuna registrazione di protocollo deve contenere, almeno, i seguenti dati obbligatori in forma non modificabile:

- ✓ il numero di protocollo, generato automaticamente dal sistema;
- ✓ la data di registrazione di protocollo, assegnata automaticamente dal sistema;
- ✓ il mittente che ha prodotto il documento;
- ✓ il destinatario del documento;
- ✓ l'oggetto del documento, da formulare in maniera tale da consentire un'intuitiva e certa identificazione del protocollo anche a posteriori;
- ✓ la classificazione del documento utilizzando le voci del Titolare;
- ✓ il riferimento al numero di protocollo del documento (o dei documenti) che ha (hanno) originato il procedimento, attraverso l'indicazione degli specifici allacci.

Come previsto dalla normativa vigente in materia di protezione dei dati personali, le UO sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

5.2.4 Trasmissione di documenti informatici

Per la spedizione all'esterno della AOO dei documenti informatici, ANAC si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dalla normativa, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche. Nello specifico, l'ANAC utilizza la casella di PEC istituzionale (protocollo@pec.anticorruzione.it).

I documenti informatici sono trasmessi per PEC, salvo il caso in cui non sia possibile risalire all'indirizzo PEC/PEO del destinatario. La trasmissione dalla casella PEC istituzionale ad una casella PEC/PEO del destinatario costituisce evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art. 47 del CAD).

Le ricevute digitali del sistema di posta elettronica certificata utilizzata per lo scambio dei documenti digitali sono associate alla spedizione.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

Per la trasmissione all'interno della AOO dei documenti informatici interni formali, ANAC utilizza le funzionalità di assegnazione e smistamento messe a disposizione dal SdP.

5.2.5 Trasmissione di documenti cartacei a mezzo posta

Nei casi in cui il destinatario sia sprovvisto di un indirizzo di PEC/PEO, il documento può essere prodotto in formato analogico (sebbene debba essere sempre sottoposto a scansione in fase di protocollazione). I mezzi di recapito della corrispondenza, in quest'ultimo caso, sono:

1. servizio di posta ordinaria o posta raccomandata;
2. consegna diretta al destinatario.

L'originale del documento trasmesso deve essere conservato dal soggetto che lo ha formato, che deve provvedere ad inserirlo nel fascicolo relativo al procedimento o questione cui si riferisce e/o ad archivarlo.

La UO, tramite il RPA, provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.

5.2.6 Fascicolazione

All'interno del SdP il RPA ha altresì la responsabilità di inserire il documento in uscita nel fascicolo relativo allo specifico procedimento nelle modalità descritte al § 9.3 "Sistema di fascicolazione dei documenti".

5.3 Matrice della responsabilità

La matrice seguente evidenzia le strutture organizzative dell'Autorità che a diverso titolo partecipano al processo disciplinato dalla presente procedura. In particolare, per ciascuna fase del processo, sono indicate le strutture organizzative coinvolte ed il relativo ruolo (Matrice RACI) con riferimento alla gestione della corrispondenza in ingresso e in uscita.

Strutture organizzative coinvolte Fase gestione corrispondenza in ingresso	Servizio di Protocollo	UO	RPA
Fase 1: ricezione e accettazione	R		
Fase 2: registrazione, segnatura e classificazione	R		R (per la classificazione di secondo livello)
Fase 3: assegnazione	R	I	
Fase 4: presa in carico	I	R	
Fase 3: sub-assegnazione	I	R	I
Fase 5: fascicolazione			R

Strutture organizzative coinvolte Fase gestione corrispondenza in uscita	Servizio di Protocollo	UO	RPA
Fase 1: Formazione e classificazione			R

Fase 2: Scansione (eventuale)		I	R
Fase 3: Registrazione e segnatura		I	R
Fase 4: Invio/Trasmissione		I	R
Fase 5: fascicolazione		I	R

Legenda: R = RESPONSABILE
 C = CONSULTATO

A = APPROVATORE
 I = INFORMATO

6. REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI RICEVUTI (IN ENTRATA)

6.1 Regole generali

Generalmente, con l'assegnazione si procede all'individuazione dell'UO competente e del destinatario interno del documento, e quindi al conferimento della responsabilità del procedimento amministrativo, mentre l'attività di smistamento consiste nel recapitare il documento protocollato e segnato all'UO medesima.

L'assegnazione può essere effettuata per competenza o per conoscenza e può essere estesa a tutti i soggetti ritenuti interessati, al fine di consentire la massima condivisione delle informazioni.

Nel caso in cui, invece, un medesimo documento afferisca a più procedimenti (ad es. di vigilanza e di precontenzioso) lo stesso viene posto in condivisione tra gli Uffici interessati, eventualmente con l'apposizione di un'annotazione nel SdP.

In particolare, il campo "annotazioni" del SdP viene utilizzato per dettagliare meglio le motivazioni dell'assegnazione di un documento a una particolare UO, per inserire note valide ai fini di un'istruttoria o per includere la motivazione in caso di rifiuto o riassegnazione di un documento da parte di una UO o le evidenze di eventuali ricerche effettuate in fase di assegnazione.

Qualora la corrispondenza riservata personale venga recapitata per errore a un diverso Ufficio, a tutela dei dati personali e/o sensibili eventualmente contenuti, va restituita integra (non vanno aperte le buste o i plichi) nella stessa giornata, al personale del Servizio di Protocollo.

All'atto dell'assegnazione il Dirigente dell'UO di competenza provvede alla presa in carico del documento e, in applicazione delle disposizioni organizzative in atto, procede alla sub-assegnazione al responsabile dell'istruttoria o RPA. Quest'ultimo verifica la corretta

classificazione del documento e la rilevanza¹ attribuite (eventualmente modificandole), inserisce il documento in apposito fascicolo elettronico con le modalità descritte nel capitolo 9 “Sistema di classificazione, fascicolazione e conservazione” e provvede alla lavorazione nei tempi previsti dai Regolamenti interni o all’archiviazione del documento.

Il SdP memorizza tutti i passaggi e successive eventuali modifiche, conservando, per ciascuno di essi, l’identificativo dell’utente che effettua l’operazione, la data e l’ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo e i conseguenti riflessi sotto il profilo della responsabilità.

I criteri e le modalità di assegnazione e smistamento dei documenti alle strutture interne, al Presidente e al Segretario Generale ANAC sono descritte nel documento “Procedure Operative Protocollo” [RIF.003].

6.2 Assegnazione e smistamento di documenti ricevuti in formato digitale

I documenti ricevuti dal Servizio di Protocollo via PEC - al termine delle operazioni di registrazione - sono assegnati e smistati all’UO competente per materia attraverso il SdP, che ne assicura la segnatura e la memorizzazione.

¹ Per rilevanza si intende l’indice di importanza (all’interno di un *range* di valori predefiniti: bassa, media, alta) che ne definisce sostanzialmente l’urgenza di trattamento e/o l’opportunità che sia posto in evidenza, in base a criteri generali definiti dall’ANAC. In sede di registrazione del documento, gli Operatori del Servizio di Protocollo provvedono appunto all’attribuzione di un criterio di rilevanza che l’UO competente può, se lo ritiene opportuno, successivamente modificare.

Il personale assegnato all'UO può visualizzare i documenti attraverso l'utilizzo del SdP, in base alle proprie abilitazioni e quindi prendere visione del contenuto del documento. Il Dirigente dell'UO ha la possibilità sub-assegnare le pratiche al personale del proprio Ufficio o, se ritenuto necessario, di archiviarle.

6.3 Assegnazione e smistamento di documenti ricevuti in formato cartaceo

Per l'assegnazione e lo smistamento dei documenti ricevuti in forma cartacea, la procedura è la seguente:

- preliminarmente l'Operatore del Servizio di Protocollo assegna e smista la corrispondenza apponendo sulla prima pagina del documento la sigla corrispondente all'UO competente per materia;
- tutti i documenti ricevuti in formato cartaceo, compresi i loro allegati e busta, sono sottoposti a scansione dal personale del Servizio di Protocollo;
- l'originale cartaceo del documento sottoposto a scansione viene consegnato all'UO di competenza;
- in caso di planimetrie o volumi non separabili si potrà comunque procedere a digitalizzare con lo scanner il frontespizio e porre l'annotazione con l'indicazione degli allegati.

6.4 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'Ufficio assegnatario deve riassegnare la comunicazione all'Ufficio ritenuto competente inserendo un'apposita annotazione sul sistema. Qualora l'Ufficio non sia in grado di provvedere autonomamente alla riassegnazione della medesima comunicazione, dovrà rifiutarlo al Servizio di Protocollo, inserendo obbligatoriamente un'annotazione contenente oltre ai motivi della propria non competenza, anche l'Ufficio ritenuto competente e/o ogni informazione ritenuta utile ai fini della corretta assegnazione. In tal caso,

l'Operatore del Servizio di Protocollo - considerata anche l'annotazione - provvederà a riassegnare il documento individuando opportunamente l'Ufficio competente.

In caso di rifiuto, qualora il nuovo assegnatario non fosse chiaramente individuabile, il RGD provvederà a sottoporre la questione al Segretario Generale dell'ANAC che fornirà le opportune indicazioni.

Dette operazioni devono essere completate di norma preferibilmente entro le quarantotto ore dalla prima assegnazione da parte del personale del Servizio di Protocollo, salvo situazioni eccezionali.

7. UO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

Il presente capitolo individua l'Unità Organizzativa responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO.

In base al modello organizzativo adottato da ANAC, nell'Allegato 3 è riportata l'articolazione della AOO in UO con evidenza dell'ufficio responsabile del servizio di protocollazione.

8. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

8.1 Documenti esclusi

Sono escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del TUDA, le seguenti tipologie documentarie:

- ✓ gazzette ufficiali;
- ✓ bollettini ufficiali PA;
- ✓ notiziari PA;
- ✓ giornali, riviste, libri;
- ✓ materiali pubblicitari;
- ✓ note di ricezione circolari;
- ✓ note di ricezione altre disposizioni;
- ✓ materiali statistici;
- ✓ atti preparatori interni;
- ✓ newsletter;
- ✓ inviti.

8.2 Documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'Allegato 4.

9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE

9.1 Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti dello Stato, delle regioni e degli enti pubblici sono beni culturali inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'ANAC, mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato e deve essere conservato nella sua organicità. L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della Direzione Generale per gli Archivi (DGA).

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta DGA.

Lo scarto dei documenti conservati nell'archivio dell'ANAC è subordinato all'autorizzazione della DGA, su proposta della Commissione di Sorveglianza, appositamente nominata. La Commissione di Sorveglianza è l'organo istituito per il controllo della corretta gestione degli archivi correnti e di deposito di ANAC, nonché per la valutazione delle proposte di scarto.

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

9.2 Sistema di classificazione dei documenti

Il sistema di classificazione dei documenti permette l'organizzazione dei documenti in funzione delle competenze dell'ANAC

Lo strumento principale è il Piano di Classificazione che rappresenta lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ANAC

Il Piano di Classificazione dell'ANAC si suddivide in voci di I livello e II livello (Titoli e Classi). Il Titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, le Classi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal Titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato. Titoli e Classi sono nel numero prestabilito dal Titolario e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito approvato dall'Amministrazione e precedentemente validato dalla DGA.

Si allega il Piano di Classificazione adottato dall'ANAC (cfr. Allegato 5).

Il Piano di Classificazione è uno strumento suscettibile di aggiornamento: esso, infatti, descrive le funzioni e le competenze dell'ANAC, soggette a modifiche in forza delle leggi e dei regolamenti.

L'aggiornamento del Piano di Classificazione compete esclusivamente al vertice dell'Amministrazione, su proposta del RGD. La revisione anche parziale del Titolario viene proposta dal RGD quando è necessario ed opportuno. Dopo ogni modifica del Titolario, il RGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche. La versione del Titolario non è retroattiva: non si applica, cioè, ai documenti protocollati prima della sua introduzione (o del suo aggiornamento) e piuttosto si fa riferimento alla versione in vigore in quello specifico momento.

Con l'attività di classificazione si organizza la documentazione secondo l'ordine logico indicato dal Piano di classificazione. Tutti i documenti ricevuti e prodotti dall'ANAC, indipendentemente dal supporto sul quale vengono formati, sono riconducibili ad una voce del Titolario vigente.

La classificazione è, dunque, l'operazione finalizzata all'organizzazione dei documenti, secondo un ordine logico, in relazione alle funzioni e alle competenze dell'ANAC

Operativamente, mediante la classificazione si assegna al documento, il codice dell'indice di classificazione (titolo e classe).

Le operazioni di classificazione vengono svolte in momenti diversi: l'addetto alla registrazione di protocollo inserisce di norma la voce di livello più alto (titolo), mentre l'attribuzione delle voci di dettaglio (classi) è demandata all'UO di competenza, tramite il RPA.

Essendo un'operazione obbligatoria, il RPA è tenuto ad indicare per ogni nuovo documento, ricevuto o prodotto, l'indice completo di classificazione corrispondente. Con riferimento alla documentazione pregressa, priva di classificazione, si è proceduto ad assegnare un indice di classificazione del *Piano di Classificazione* in vigore alla data di produzione del documento.

9.3 Sistema di fascicolazione dei documenti

Ogni documento, dopo la classificazione, viene inserito a cura dell'UO (tramite il RPA) nel fascicolo di riferimento.

Il fascicolo è lo strumento che consente l'aggregazione dei documenti in base al procedimento o allo specifico "affare" e al suo interno i documenti sono archiviati secondo l'ordine cronologico di registrazione.

La fascicolazione viene gestita attraverso le funzioni ad essa dedicate nel SdP. Il sistema di protocollo informatico fornisce «le informazioni sul collegamento esistente tra ciascun documento ricevuto e i documenti formati nell'adozione del provvedimento finale» (TUDA art. 52 c.1c) nonché «garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato» (TUDA art. 52 c.1f).

Quando un nuovo documento viene recapitato all'ANAC, l'UO assegnataria stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo, se il documento stesso debba essere collegato a un procedimento o specifica questione in corso e, pertanto, debba essere inserito in un fascicolo esistente oppure se il documento si riferisce a un nuovo procedimento o questione per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- a) se il documento si ricollega ad un procedimento o questione in corso, l'addetto dell'UO competente:
 - seleziona il relativo fascicolo;
 - collega la registrazione di protocollo del documento al fascicolo selezionato;
- b) se il documento dà avvio ad un nuovo fascicolo, il soggetto preposto:
 - esegue l'operazione di apertura del fascicolo;
 - collega la registrazione di protocollo del documento al nuovo fascicolo aperto.

L'operazione di "apertura" di un nuovo fascicolo comprende la registrazione di alcune informazioni essenziali, quali:

- ✓ oggetto del fascicolo;
- ✓ ufficio titolare del procedimento;
- ✓ indice di classificazione (titolo e classe);
- ✓ numero del fascicolo (assegnato automaticamente dal sistema di protocollo);
- ✓ data di apertura del fascicolo.

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. La chiusura del fascicolo viene formalizzata utilizzando la funzione del sistema di protocollo corrispondente allo stato "agli Atti".

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

9.4 Archivio analogico dell'ANAC

9.4.1 Versamento dei fascicoli nell'archivio di deposito

Periodicamente il RC provvede a trasferire i fascicoli analogici relativi ai procedimenti conclusi nella sezione di deposito dell'archivio generale.

Per una regolare e costante “alimentazione” dell’archivio di deposito il RC stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli dagli archivi correnti dei diversi UO dell’ANAC all’archivio di deposito. La regolare periodicità dell’operazione è fondamentale per garantire l’ordinato sviluppo dell’archivio di deposito. Il trasferimento deve essere attuato rispettando l’organizzazione che i fascicoli avevano nell’archivio corrente.

Il processo di versamento si articola in più fasi. Una prima fase riguarda il trasferimento fisico della documentazione presso un locale della sede dell’Amministrazione, appositamente dedicato alla custodia temporanea della documentazione, in cui il materiale documentario viene verificato per accertare la sua idoneità ad essere trasferito all’archivio di deposito per la custodia di lungo periodo. Una seconda fase riguarda il conferimento fisico della documentazione presso i locali dell’archivio di deposito vero e proprio con relativo trasporto e messa a dimora delle scatole che contengono la documentazione da custodire.

In tal senso, prima di effettuare il versamento di cui sopra, il RPA procede alla verifica:

- ✓ dell’effettiva conclusione ordinaria della pratica;
- ✓ della corretta indicazione della data di chiusura del fascicolo.

Il RPA è tenuto inoltre:

- ✓ allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l’eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- ✓ a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l’accesso organico.

Ricevuti i fascicoli, il RC predispone un elenco di “versamento” e fa eseguire un controllo del materiale riversato. Il RC è tenuto ad accettare soltanto i fascicoli con materiale ordinato e completo. Copia dell’elenco di versamento “definitivo” viene conservata dal RC.

Il fascicolo che in sede di controllo presenta delle incongruenze deve essere restituito agli UO tenutari dell’archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie.

Nell'eventualità che non sia possibile risolvere le incongruenze, l'UO deposita il fascicolo dichiarando ufficialmente la mancanza e si assume la responsabilità della trasmissione agli atti.

Per quanto riguarda il processo di conservazione a cui vengono sottoposti i documenti amministrativi informatici dell'ANAC si rimanda al relativo Manuale di conservazione reperibile sul sito istituzionale dell'Autorità.

9.4.2 Consultazione e movimentazione dell'archivio corrente, di deposito e storico

La richiesta di consultazione, e di conseguenza la movimentazione dei fascicoli, può pervenire dall'interno dell'ANAC, oppure da utenti esterni con diritto di accesso ai documenti, per scopi giuridico-amministrativi o per scopi storici.

9.4.2.1 Consultazione da parte di personale interno ad ANAC

Le UO, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nell'archivio di deposito.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa, contenente gli estremi identificativi della documentazione richiesta e il nominativo del richiedente. Il servizio prevede la possibilità di consultare la documentazione in originale analogico (con consegna della stessa e successiva restituzione) o in copia digitale (con consegna di una versione digitale frutto di una scansione dell'originale analogico). La richiesta e la consultazione avviene con il supporto di un portale web messo a disposizione dal SGD.

Tale movimentazione viene registrata a cura del RC in un apposito registro (anche informatico) di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata. Il RC verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

In caso di consultazione di un originale cartaceo, l'affidatario dei documenti è tenuto a non estrarre i documenti originali dal fascicolo, né ad alterare l'ordine degli stessi rispettandone la sedimentazione archivistica e il vincolo archivistico.

Nel caso di consultazione degli archivi originali digitali, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'ANAC nel Manuale della Conservazione digitale.

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

9.4.2.2 Consultazione da parte di personale esterno all'Amministrazione

La domanda di accesso ai documenti viene presentata formalmente ad ANAC, attraverso la casella istituzionale e trasmessa alla UO competente, che provvede (in caso di diritto di accesso ai sensi del *Regolamento di Accesso agli Atti*) ad inoltrarla al servizio di gestione dell'archivio così come descritto nel paragrafo precedente. Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.

Il RC provvede alla gestione delle operazioni di consultazione conformemente ai criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

L'ingresso all'archivio di deposito e storico, è consentito solo agli addetti del servizio di gestione dell'archivio. La consultazione dei documenti originali analogici è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'Amministrazione.

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il RC rilascia apposita dichiarazione.

9.4.3 Scarto dei documenti

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

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

ANAC ha predisposto un Piano di Conservazione (Allegato 5) che indica per ogni voce del Titolario il periodo di conservazione rispetto alla data di chiusura del fascicolo di riferimento.

Le operazioni di selezione e scarto sono effettuate periodicamente, sotto la vigilanza del RC, a cura degli addetti del servizio di gestione dell'archivio e si basano sulla produzione e validazione di una "proposta di scarto" validata dalla Commissione di Sorveglianza.

10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

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

10.1 Unicità del protocollo informatico

Nell'ambito dell'A00 il registro di protocollo è unico ed è gestito dal Servizio di Protocollo.

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 registro è generato automaticamente dal SdP che attribuisce a ciascun documento registrato il numero e la data di protocollazione. Ai sensi dell'art. 57 del TUDA il numero di protocollo è costituito da almeno sette cifre numeriche ed è rinnovato ogni anno solare.

La numerazione delle registrazioni di protocollo è unica e progressiva; si conclude il 31 dicembre di ogni anno ed inizia il 1 gennaio dal numero 0000001.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale o informatica di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se collegati tra loro.

Il protocollo fa fede, anche con valore giuridico, dell'effettivo ricevimento e spedizione di un documento, pertanto, la documentazione non registrata presso il Servizio di Protocollo viene considerata giuridicamente inesistente presso l'ANAC.

10.2 Registro giornaliero di protocollo

Il registro giornaliero di protocollo si genera quotidianamente, mediante produzione automatica, su supporto informatico, ed è costituito dall'elenco dei protocolli registrati nell'arco di un giorno e delle informazioni ad essi connesse. Al fine di garantire l'immodificabilità del contenuto, il registro giornaliero di protocollo prodotto viene a sua volta protocollato e rappresenta generalmente il primo protocollo del giorno successivo. Inoltre, ai sensi della normativa vigente, il registro giornaliero di protocollo viene trasmesso entro la giornata lavorativa successiva al sistema di conservazione dei documenti.

10.3 Registrazione di protocollo dei documenti

Su ogni documento ricevuto o spedito dall'ANAC è effettuata la registrazione di protocollo con il SdP, consistente nella memorizzazione dei dati obbligatori previsti dalla norma. Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, ai sensi dell'art. 53 del TUDA, i seguenti dati obbligatori in forma non modificabile:

- a. il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b. la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c. il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- d. l'oggetto del documento, registrato in forma non modificabile;
- e. la data e il numero di protocollo del documento ricevuto, se disponibili;

- f. l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

La protocollazione della corrispondenza ricevuta segue di norma l'ordine cronologico di arrivo della stessa, ad eccezione delle comunicazioni che ad un primo esame del personale del Servizio di Protocollo suggeriscono la necessità di essere gestite con particolare urgenza.

10.4 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione e avviene attraverso l'apposizione sul documento di un "segno" grafico (realizzato attraverso la stampa di un codice a barre contenente gli estremi di registrazione del protocollo o per i documenti cartacei con una etichetta autoadesiva corredata del medesimo codice a barre) sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- ✓ codice identificativo o nome per esteso dell'ANAC;
- ✓ data e numero di protocollo del documento.

Essa consente di individuare ciascun documento in modo inequivocabile, associando all'originale del documento, in forma permanente non modificabile, le informazioni riguardanti il documento stesso.

L'operazione di segnatura dei documenti ricevuti in formato cartaceo viene effettuata dal personale del Servizio di Protocollo successivamente all'acquisizione del documento in formato elettronico. La segnatura di protocollo viene apposta sulla prima pagina del documento.

Tutti i documenti pervenuti, indipendentemente dal canale in ingresso, una volta registrati (ed eventualmente scansionati preliminarmente, se cartacei), sono automaticamente sottoposti a segnatura dal SdP. I dati della segnatura di protocollo di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche

dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) reso disponibile dagli organi competenti.

Le informazioni incluse nella segnatura sono le seguenti:

- ✓ codice identificativo dell'Amministrazione;
- ✓ codice identificativo dell'AOO;
- ✓ codice identificativo del registro;
- ✓ data e numero di protocollo del messaggio ricevuto o inviato;
- ✓ oggetto;
- ✓ mittente;
- ✓ destinatario/destinatari.

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

L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto come descritto nel § 5.1.1.1 "Ricezione dei documenti informatici".

10.5 Annullamento delle registrazioni di protocollo

I dati obbligatori relativi alla registrazione di protocollo non sono modificabili. La necessità di effettuare eventuali modifiche comporta l'obbligo di annullare l'intera registrazione di protocollo.

Solo il RGD, sentito eventualmente il Presidente e/o il Segretario Generale, è autorizzato ad annullare ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. L'annullamento di una registrazione di protocollo deve essere richiesto con specifica e-mail, adeguatamente motivata, indirizzata alla casella di supporto di riferimento e solo a seguito della valutazione della particolare questione, il RGD può autorizzare l'annullamento stesso.

Ai sensi degli artt. 54 del TUDA, i dati annullati e/o modificati rimangono memorizzati nella procedura del protocollo informatico unitamente alle informazioni relative all'ora, alla data e al nominativo dell'utente che effettua l'operazione.

10.6 Livello di riservatezza

Ove si renda necessario garantire un alto grado di riservatezza delle informazioni è disponibile all'interno del SdP dell'Autorità una specifica funzionalità che consente la gestione di un livello di riservatezza, che non rende disponibile il documento alla consultazione dei soggetti non espressamente abilitati.

10.7 Casi particolari di registrazioni di protocollo

Le modalità di gestione della corrispondenza riservata, di quella che, in relazione al contenuto o all'identità del mittente, appare di particolare rilievo per l'Autorità, nonché di quei documenti in ingresso soggetti a forme particolari di registrazione (documentazione relativa a gare d'appalto o concorsi, documenti sottoposti a protocollazione automatica o acquisiti attraverso specifici sistemi dell'ANAC), sono disciplinate come di seguito indicato.

10.7.1 Corrispondenza riservata

I documenti soggetti alla procedura di riservatezza sono i seguenti:

- ✓ atti dei procedimenti amministrativi in relazione ai quali sussistano particolari esigenze di protezione della riservatezza di terzi, persone, gruppi, imprese ed associazioni e dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;

- ✓ atti contenenti informazioni classificate o coperte da segreto di Stato;
- ✓ documenti relativi a vicende di persone o a fatti privati o particolari;
- ✓ documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- ✓ tipologie di documenti individuati dall'art. 24 della *Legge sul procedimento amministrativo*;
- ✓ documenti che contengano dati sensibili, giudiziari o personali, come definiti dal Codice in materia di protezione dei dati personali;
- ✓ documenti afferenti a segnalazioni di cui all'art. 54 bis d.lgs. n. 165/2001 e smi ("whistleblowers").

La selezione della casella "riservato" sul SdP, nei casi sopra previsti, rende la protocollazione riservata e visibile esclusivamente all'utente che ha proceduto alla registrazione e all'assegnatario.

Va evidenziato che la procedura di cui sopra consente di eseguire sul documento c.d. "riservato" tutte le operazioni quali: la registrazione, la segnatura, la classificazione e la fascicolazione, adottate per gli altri documenti e procedimenti amministrativi. In caso di documento analogico va comunque eseguita la scansione ai fini della conservazione dello stesso in formato elettronico.

Il particolare carattere di "riservatezza" può essere attribuito ad una comunicazione anche in un momento successivo alla registrazione, consentendo anche agli assegnatari di renderlo "riservato" nel corso del flusso di lavorazione.

10.7.2 Documenti indirizzati nominalmente al personale dell'ANAC

La posta indirizzata nominalmente al personale dell'ANAC è regolarmente aperta e registrata dal personale del Servizio di Protocollo, a meno che sulla busta non sia riportata la dicitura "personale", "riservata personale" o espressione equivalente.

In questo caso la corrispondenza viene consegnata in busta chiusa al destinatario che, se reputa che i documenti acquisiti debbano essere protocollati, provvede a trasmetterli al Servizio di Protocollo.

10.7.3 Corrispondenza di particolare rilevanza

I documenti in ingresso vengono assegnati alle UO *ratione materiae* con l'indicazione del grado di rilevanza del documento. In fase di protocollazione, sulla base dell'analisi eseguita sul contenuto della comunicazione oggetto di registrazione, l'Operatore del Servizio di Protocollo esegue una pre-assegnazione del grado di rilevanza del documento, attribuendogli uno dei seguenti valori predefiniti: ALTA, MEDIA e BASSA.

L'UO competente, ricevuta la documentazione, verifica la corretta attribuzione della rilevanza pre-assegnata e, qualora lo ritenga necessario, procede alla sua modifica assegnando il valore ritenuto più congruente per il documento in esame.

I criteri e le modalità di assegnazione del grado di rilevanza del documento sono descritti nel documento "Procedure Operative Protocollo" [RIF.003].

10.7.4 Corrispondenza relativa a gare d'appalto o concorsi

La corrispondenza relativa a bandi di gara non viene aperta, piuttosto viene registrata e consegnata chiusa direttamente all'Ufficio competente.

Nel caso tale tipologia di corrispondenza sia consegnata direttamente a mano dall'interessato o da persona da questi delegata, viene acquisita al momento della presentazione, dando ricevuta dell'avvenuta consegna.

10.7.5 Documentazione acquisita attraverso specifici sistemi ANAC

Atti, documenti e comunicazioni utilizzati ai fini dell'abilitazione (ad esempio: dichiarazioni sostitutive di atto notorio trasmessi per la registrazione) o dell'utilizzo dei servizi informatici resi disponibili sul portale ANAC sono già acquisiti e tracciati su apposite piattaforme che ne curano la registrazione nell'ambito di appositi repertori, attribuendo loro un codice univoco e la persistenza nel tempo. Pertanto, tali tipologie di atti non sono oggetto di registrazione al protocollo (vedi § 8.2 Documenti soggetti a registrazione particolare). Esulano da tale insieme le segnalazioni di vigilanza inoltrate tramite il modulo web come descritto al § 5.1.1.1 "Ricezione dei documenti informatici".

10.7.6 Documenti anonimi o non firmati

I documenti anonimi sono regolarmente sottoposti alle operazioni di registrazione di protocollo e di segnatura e nel campo «mittente» viene apposta la dicitura "anonimo". Tali documenti vanno assegnati all'UO competente per materia. Nel caso si tratti di segnalazioni vale quanto descritto nel § 5.1.1 "Ricezione dei documenti informatici".

10.7.7 Documenti con più destinatari

Disposizioni generali, ordini di servizio e tutte le altre comunicazioni interne che abbiano più destinatari si registrano con un solo numero di protocollo generale.

10.7.8 Protocollazione di un numero consistente di documenti

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione al Servizio di Protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

10.7.9 Protocolli urgenti

Il RGD può disporre la protocollazione immediata di documenti in entrata – in deroga alla normale gestione secondo l'ordine cronologico di arrivo della corrispondenza – nel caso in cui il carattere d'urgenza si evinca dal contenuto del documento stesso.

10.7.10 Integrazioni documentarie

In caso di acquisizione al Servizio di Protocollo di integrazioni documentali, il personale addetto non è tenuto a verificare la completezza sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati allacciandolo al/ai protocollo/i originale/i.

Tale verifica spetta al RPA che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando di inviarli alla casella istituzionale ANAC e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati sul protocollo a cura del SGD con appositi allacci e annotazioni.

10.7.11 Messaggi di Posta Elettronica Ordinaria

Le caselle di posta elettronica convenzionale in uso alle UO sono presidiate dagli stessi che valutano, di volta in volta, se è necessario inoltrare alla casella PEC istituzionale la specifica comunicazione ai fini della sua protocollazione da parte degli addetti al Servizio di Protocollo. In generale, tenuto conto che il sistema di posta elettronica non certificata non consente la certa identificazione del mittente, questa tipologia di corrispondenza è trattata come di seguito descritto:

- ✓ in caso di acquisizione di un documento fornito di firma digitale, l'atto viene valutato alla stregua di un documento elettronico inviato con qualunque mezzo di posta;
- ✓ in caso di acquisizione di un documento scansionato e dotato di firma autografa resta fermo l'onere in capo al RPA della verifica della sicura provenienza del documento; in caso, poi, di mittente non verificabile, il RPA valuta discrezionalmente l'opportunità di utilizzare o meno il documento così pervenuto.

11. DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO

La descrizione completa delle funzionalità dell'applicativo di protocollo è disponibile e consultabile insieme al documento di procedure operative di funzionamento del protocollo nella intranet dell'ANAC

12. MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA

Nel caso di interruzioni del funzionamento del SdP per cause tecniche accidentali o programmate, che impediscano la regolare erogazione del SGD, ai sensi dell'art. 63 del Testo Unico, le registrazioni di protocollo vengono effettuate su un registro di emergenza.

In particolare, il RGD autorizza con proprio provvedimento la compilazione del registro di emergenza in forma cartacea oppure in forma digitale e, al ripristino della funzionalità del SGD, tutte le registrazioni effettuate vengono inserite a sistema, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema di protocollo.

Qualora l'interruzione del funzionamento del sistema di protocollo si prolunghi per più di ventiquattro ore, il RGD, ai sensi della normativa vigente, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle informazioni di cui sopra, vengono riportati gli estremi del provvedimento di autorizzazione.

Quando viene ripristinata la piena funzionalità del sistema, il RGD o un suo delegato provvede alla chiusura del registro di emergenza, annotando sullo stesso il numero delle registrazioni effettuate, la data e l'ora di ripristino della funzionalità del sistema.

13. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

13.1 Modalità di approvazione e aggiornamento del manuale

L'ANAC adotta il presente "Manuale di gestione" su proposta del RGD, sentita la DGA. Il responsabile dell'aggiornamento del presente Manuale è il RGD.

Il presente manuale potrà essere aggiornato a seguito di:

- ✓ normativa sopravvenuta;
- ✓ introduzione di nuove pratiche finalizzate a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- ✓ inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Le modifiche apportate ai soli allegati del presente Manuale obbligano alla ri-emissione e aggiornamento dello stesso.

Tutte le strutture organizzative dell'Autorità, pertanto, devono segnalare tempestivamente al Servizio di Protocollo 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 della procedura stessa.

13.2 Pubblicità del presente Manuale

Il presente Manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento. Copia del presente Manuale è:

- ✓ resa disponibile a tutto il personale dell'ANAC sulla intranet dell'Autorità;
- ✓ pubblicato sul sito istituzionale dell'Amministrazione.

ALLEGATI

Allegato 1 – Elenco sintetico formati accettati

Allegato 2 – Scheda informativa oggetti documentali

Allegato 3 – Articolazione della AOO

Allegato 4 – Elenco documenti soggetti a registrazione particolare

Allegato 5 - Piano di classificazione, conservazione e fascicolazione dei documenti (Titolario e Massimario di selezione e scarto dell'archivio dell'ANAC)