

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CONSIGLIO PER LA RICERCA IN AGRICOLTURA E L'ANALISI DELL'ECONOMIA AGRARIA

EMISSIONE DEL DOCUMENTO

Autori

Riferimento	Nome
Prot. 5785 del 23/01/2023	Adele Parrella (CREA-UG8), Mara Sarlatto (CREA-STs), Giuseppe Luigi Barreca (CREA-DC)
Prot. 24648 del 01/04/2025	Fabio Palpini (CREA-UG8), Adele Parrella (CREA-UG8), Antonio Di Mezza (CREA-USA1), Adele Trombetta (CREA-UG4)

Revisioni

Versione	Data	Descrizione	Nome
0.2	19/04/2024	Approvato	Luca Erba, Valentina Longo
1.0	30/05/2024	Approvato	CDA
1.1	04/02/2026	Approvato	Luca Erba

Registro delle Revisioni

Versione	Modifiche apportate
1.0	Documento redatto in ottemperanza a quanto previsto dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate dall'AgID, ed. Maggio 2021.
2.0	Inseriti riferimenti alle seguenti tematiche: realizzazione dei diagrammi di flusso dei documenti in entrata e uscita; descrizione modalità chiusura e riapertura fascicoli in conservazione; descrizione modalità di backup sistema documentale; descrizione delle modalità in riservatezza della protocollazione; gestione delle utenze del sistema Documentale.

Allegati

Nome Documento	Versione	Scopo
Allegato 1	Decreto del Direttore Generale n.109 del 20 dicembre 2012	Titolario CREA - Piano di classificazione del CREA
Allegato 2	Delibera del CdA n. 16 del 24 gennaio 2013	Massimario di conservazione e scarto dei documenti del CREA (prima CRA)

Sommario

1. Principi generali	7
Premessa.....	7
Ambito di applicazione del manuale.....	7
Definizioni e norme di riferimento	8
Aree Organizzative Omogenee	12
Servizio per la gestione informatica del protocollo	12
Conservazione delle copie di riserva	13
Tutela dei dati personali.....	13
Caselle di Posta elettronica	13
Sistema di classificazione dei documenti.....	13
Formazione.....	13
Accreditamento dell'AOO all'IPA	13
Dematerializzazione dei procedimenti amministrativi della AOO	14
2. Eliminazione dei registri di protocollo diversi dal Registro ufficiale di protocollo informatico 15	
Piano di attuazione	15
3. Piano di Sicurezza.....	15
Obiettivi del piano di sicurezza.....	15
Generalità.....	15
Misure di sicurezza	16
Abilitazioni all'utilizzo delle funzionalità del prodotto di protocollo informatico.....	16
Riservatezza dei documenti di Protocollo.....	17
Backup Sistema.....	18
Formazione dei documenti – Aspetti attinenti alla sicurezza	18
Gestione dei documenti informatici.....	18
Trasmissione ed interscambio dei documenti informatici	19
Accesso ai documenti informatici.....	19
Utenti interni alla AOO.....	20
Accesso al registro di protocollo per utenti interni alla AOO.....	20
Utenti esterni alla AOO - Altre AOO/Amministrazioni	21
Utenti esterni alla AOO – Privati.....	21

Conservazione dei documenti informatici	21
4. Modalità di utilizzo di strumenti informatici per la formazione e lo scambio dei documenti informatici.....	22
Il documento analogico – cartaceo.....	22
Documenti ricevuti.....	23
Documenti inviati.....	23
Documenti interni formali.....	24
Documenti interni informali.....	24
Formazione dei documenti informatici– Aspetti operativi	24
Formazione dei documenti informatici amministrativi – Aspetti operativi.....	25
Sottoscrizione dei documenti informatici	26
Requisiti degli strumenti informatici di scambio	26
Firma digitale e firma elettronica.....	27
Verifica delle firme SdP per i formati .p7m.....	28
Uso posta elettronica certificata	29
5. Descrizione del flusso di lavorazione dei documenti.....	30
Generalità.....	30
Flusso dei documenti in ingresso alla AOO.....	30
Flusso dei documenti in uscita dalla AOO.....	33
Procedure per la gestione dei documenti in uscita (flow chart).....	33
6. Regole di assegnazione dei documenti ricevuti	34
Regole disponibili con il SdP.....	34
Attività di assegnazione	35
Corrispondenza di particolare rilevanza	35
Assegnazione dei documenti ricevuti in formato digitale.....	35
Assegnazione dei documenti ricevuti in formato cartaceo	35
Modifica delle assegnazioni.....	36
7. Regole di assegnazione dei documenti inviati	36
8. Elenco dei documenti esclusi dalla registrazione di protocollo e documenti soggetti a registrazione particolare	36
Documenti esclusi.....	36
Documenti soggetti a registrazione particolare.....	37
9. Sistema di classificazione, fascicolazione e piano di conservazione.....	37

Protezione e conservazione degli archivi pubblici.....	37
Titolario o piano di classificazione	38
Fascicoli e Dossier	39
Fascicoli del personale	41
Consultazione e movimentazioni dell'archivio corrente, di deposito e storico	42
Consultazione.....	43
Apertura di un fascicolo chiuso	43
10. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico	44
Unicità del protocollo informatico	44
Registro giornaliero di protocollo	44
Registrazione di protocollo	44
Elementi facoltativi delle registrazioni di protocollo.....	45
Segnatura di protocollo dei documenti	45
Annullamento delle registrazioni di protocollo	46
Livello di riservatezza.....	46
Casi particolari di registrazione di protocollo	47
Gestione delle registrazioni di protocollo con SdP	47
Registrazioni di protocollo.....	47
11. Descrizione delle funzioni e delle modalità operative del sistema di protocollo informatico	47
Descrizione funzionale ed operativa	47
Rilascio delle credenziali di autenticazione e dei profili di autorizzazione.	47
Operatore Ufficio di protocollo.....	48
12. Modalità di utilizzo del registro di emergenza.....	48
Il registro di emergenza.....	48
Modalità di apertura del Registro di Emergenza	48
Modalità di utilizzo del Registro di Emergenza.....	48
Modalità di chiusura e di recupero del Registro di Emergenza	49
13. Approvazione e aggiornamento del manuale, regole transitorie e finali	49
Modalità di approvazione ed aggiornamento del manuale	49
Regolamenti abrogati	49
Pubblicità del presente manuale.....	49
Operatività del presente manuale	49

Norme di rinvio.....	49
----------------------	----

1. PRINCIPI GENERALI

Premessa

Il Manuale di gestione del protocollo informatico, dei documenti e dell'archivio del CREA, d'ora in avanti manuale, è lo strumento con cui il CREA descrive la politica adottata nella gestione dei documenti, analogici e digitali. Il manuale, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Il presente manuale è adottato ai sensi delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici a cura dell'Agenzia per l'Italia Digitale (Agid), entrate in vigore il 1° gennaio 2022.

Secondo le Linee guida, il manuale di gestione “descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi”

In particolare, individua:

- gli strumenti, i sistemi informativi e i formati adottati per la formazione e lo scambio dei documenti informatici;
- le scelte operate rispetto alla gestione della sicurezza e della continuità operativa (piano di sicurezza);
- i flussi di lavorazione dei documenti;
- le regole da seguire per l'assegnazione dei documenti ricevuti e inviati;
- i piani di classificazione e di fascicolazione;
- il piano di conservazione;
- le modalità di produzione e di conservazione delle registrazioni di protocollo informatico;
- le modalità di utilizzo del registro di emergenza.

Il manuale è uno strumento operativo, flessibile e aggiornato in grado di promuovere la condivisione, senza imporre vincoli rigidi e inutili, è realmente utile ed utilizzabile dagli operatori del protocollo informatico e da tutti i dipendenti del CREA. Sono previsti periodici aggiornamenti che tengano conto anche delle effettive applicazioni a tutti i contesti organizzativi del CREA.

Ambito di applicazione del manuale

Il manuale è lo strumento con cui viene descritto e disciplinato il sistema di gestione dei documenti. La gestione documentale è la funzione di organizzazione e controllo esercitata dall'amministrazione sulla propria documentazione al fine di disporre del necessario supporto informativo e documentario per lo svolgimento efficiente delle attività, sia a fini interni che a fini di trasparenza amministrativa. Le finalità della gestione documentale all'interno di una Pubblica Amministrazione (d'ora avanti PA) sono:

- produrre con qualità e senza ridondanza i documenti necessari ed efficaci per l'espletamento dell'attività propria dell'ente in qualunque contesto tecnologico;
- organizzare i documenti in modo che siano facilmente recuperabili e utilizzabili nella gestione amministrativa;

- conservare i documenti prodotti in modo che essi mantengano la loro capacità probatoria.

La tenuta di un corretto sistema di gestione documentale richiede lo svolgimento delle seguenti attività:

1. **registrazione dei documenti:** i documenti devono essere identificati con certezza al momento della loro formazione attraverso la registrazione, in modo da garantire la loro identità (provenienza, univocità, data certa, integrità dei contenuti);
2. **classificazione dei documenti:** le relazioni tra documenti, formati o ricevuti, devono essere funzionali, stabili e non arbitrarie al fine di riflettere il flusso di lavoro e di accumulazione;
3. **formazione dei fascicoli:** classificare non basta poiché è necessario assicurare che i documenti relativi allo stesso procedimento siano sempre connessi, e pertanto, recuperabili e verificabili;
4. **valutazione, selezione e scarto:** attività che garantisce l'efficienza del sistema, evitando la ridondanza e la duplicazione dei documenti. Lo scarto, per essere efficace, deve essere collegato alle attività di classificazione e di formazione dei fascicoli;
5. **regolamentazione interna:** attività che permette uniformità nella produzione e trasmissione dei documenti e che acquisisce una particolare rilevanza nel contesto.

Definizioni e norme di riferimento

Che cos'è e a cosa serve

Il Manuale di gestione documentale è uno strumento operativo che descrive le procedure e le istruzioni per la corretta formazione, gestione e conservazione della documentazione ricevuta, inviata, o comunque prodotta, dall'amministrazione, secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolazione, reperimento e conservazione dei documenti.

Norme di riferimento

Il Manuale di gestione è adottato ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, nel rispetto della ulteriore legislazione:

- Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Direttiva del Presidente del Consiglio dei Ministri 28 ottobre 1999, Gestione informatica dei flussi documentali nelle pubbliche amministrazioni;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, d'ora in avanti "TUDA";
- Decreto del Presidente della Repubblica 8 gennaio 2001, n. 37, Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;

- Decreto legislativo 22 gennaio 2004, n. 42, Codice dei beni culturali e s.m.i., con specifico riferimento alle norme relative alla corretta formazione e conservazione degli archivi correnti e di deposito delle PA;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale e s.m.i., d'ora in avanti "CAD";
- Decreto della Presidente del Consiglio dei Ministri 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto della Presidente del Consiglio dei Ministri 21 marzo 2013, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Regolamento UE 2014/910 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE detto anche "Regolamento eIDAS" (electronic IDentification Authentication and Signature);
- Reg. UE 2016/679 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, d'ora in avanti "Regolamento";
- Decreto legislativo 10 agosto 2018 n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* pubblicate dall'Agid (ed. maggio 2021).

Le Linee Guida Agid si applicano dal 1° gennaio 2022, a partire da tale termine i soggetti di cui all'art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle Linee Guida Agid.

A partire dalla data di applicazione delle Linee Guida Agid, sono stati abrogati:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";

• il DPCM 3 dicembre 2013, contenente “Regole tecniche in materia di sistema di conservazione”.
Per quanto concerne il DPCM 3 dicembre 2013, contenente Regole tecniche per il protocollo informatico, a partire dalla data di applicazione delle Linee guida Agid sono abrogate tutte le disposizioni fatte salve le seguenti prescrizioni:

- 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.

Sempre a far data dalla data di applicazione delle Linee guida Agid, la circolare n. 60 del 23 gennaio 2013 dell'Agid in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni” è abrogata e sostituita dall'allegato 6 “Comunicazione tra AOO di documenti amministrativi protocollati” del presente documento.

Definizioni

La gestione documentale è l'insieme delle attività finalizzate al trattamento dei documenti formati e acquisiti dal CREA in modo da garantirne la **certezza documentale**, l'**assegnazione** alla Struttura competente e l'**ordinata conservazione**.

La **certezza documentale** consiste nel garantire, per ciascun documento:

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

L'**assegnazione** consiste nell'attribuzione di ciascun documento alle unità organizzative competenti per la trattazione del procedimento amministrativo o affare, cui il documento si riferisce. L'**ordinata conservazione** consiste nelle attività volte a garantire la conservazione e il reperimento dei documenti attraverso la classificazione e la fascicolazione degli stessi.

Il documento amministrativo è qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una PA e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica. Il documento amministrativo può assumere la forma di documento informatico o analogico.

L'Unione europea è intervenuta nel 1999 con una Direttiva e nel 2014 con un Regolamento di cui si è tenuto conto nei decreti correttivi del CAD. In particolare, sono stati definiti i concetti di documento elettronico e informatico.

Il documento elettronico è qualsiasi contenuto conservato in forma elettronica, in particolare testo, registrazione sonora, visiva o audiovisiva.

Il legislatore italiano ha recepito il concetto di documento elettronico, specificando che il documento informatico è “documento giuridicamente rilevante” all’interno della categoria di documento elettronico.

L’aggettivo informatico qualifica il documento in base al fatto che sia scritto (memorizzato) su un supporto informatico (e non su carta o su altro supporto analogico) e che contenga informazione codificata con un linguaggio convenzionale in bit.

Il documento analogico è definito per differenza: “rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti”.

Per esercitare la propria funzione il documento richiede strumenti e procedure finalizzati ad assicurare affidabilità e accuratezza nella sua produzione e autenticità nella sua tenuta e conservazione.

È indispensabile, a tal fine, individuare le componenti costitutive del documento, che ne determinano il valore giuridico e ne consentono la verifica nel tempo.

Sul piano generale un documento presenta alcuni elementi costitutivi che derivano dalla sua funzione originaria di dare certezza:

- provenienza certa, da non confondere con l’indirizzo di provenienza o trasmissione, ma intesa come origine/assunzione di paternità: si tratta della indicazione certa e verificabile dell’autore del documento in quanto responsabile per il suo contenuto. In quanto riconducibile alla volontà di una persona fisica, il documento è sempre una dichiarazione di rappresentazione e richiede che l’identità dell’autore sia accertabile;
- data certa della sua formazione (del momento in cui si è espressa la volontà dell’autore);
- contenuto stabile (verificabile nella sua integrità).

La registrazione dei documenti assume un ruolo centrale per il trattamento dei documenti informatici.

Il protocollo informatico consente di rispondere con efficacia all’esigenza primaria di mantenere la capacità probatoria dei documenti informatici, poiché assicura la provenienza dei documenti (in termini di imputabilità del contenuto al suo autore) e la loro integrità e ne rende possibile la verifica.

La segnatura di protocollo per i documenti informatici della PA consente di assicurare validazione temporale ai documenti soggetti a registrazione di protocollo, poiché il sistema di registrazione identifica ogni documento con un numero progressivo correlato in modo non modificabile alla data della registrazione e a una serie di elementi identificativi obbligatori del documento stesso, inclusa l’impronta (risultato della funzione di hash) del documento informatico.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- AOO – Area Organizzativa Omogenea;
- CGD – Coordinatore della Gestione Documentale;
- GO – Gruppo di Organigramma – Ufficio della UOR che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario ultimo del documento.
- MdG – Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- PG – Protocollo Generale;
- RPA – Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell’esecuzione degli adempimenti amministrativi;

- RSP – Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- SdP – Servizio di protocollo informatico;
- UOR – Uffici Organizzativi di Riferimento – un insieme di uffici (GO) che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- UU – Ufficio Utente – un gruppo di utenti che svolgono la stessa attività;
- UOP – Unità Organizzativa di registrazione di Protocollo (UOP).

Aree Organizzative Omogenee

Per la gestione dei documenti l'Amministrazione ha istituito un'unica AOO nell'ambito della quale è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'interno dell'amministrazione il sistema archivistico è unico, il sistema di protocollazione è centralizzato, tutta la corrispondenza, in ingresso e in uscita, è gestita dalle singole UOR.

Servizio per la gestione informatica del protocollo

Nella AOO il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi è assegnato al GO Protocollo Generale (PG) presso la UOR di appartenenza.

Al suddetto servizio è preposto un dirigente nominato RSP.

In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del RSP:

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;
- abilitare gli utenti dell'AOO all'utilizzo del SdP e definire per ciascuno di essi il tipo di funzioni più appropriate tra quelle disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnature di protocollo;
- garantire la corretta conservazione della copia del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili nel SdP.

Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, è garantita la non modificabilità delle operazioni di registrazione e, al termine della giornata lavorativa, il contenuto del registro giornaliero di protocollo, viene inviato in conservazione.

Tutela dei dati personali

L'Amministrazione, titolare dei dati di protocollo e dei dati personali, contenuti nella documentazione amministrativa di propria competenza, adegua il trattamento alle prescrizioni del Regolamento (UE) 2016/679 e del D.Lgs.196/2003, così come modificato dal decreto legislativo 10 agosto 2018, n. 101 contenente disposizioni per l'adeguamento nazionale al Regolamento (UE) 2016/679.

Caselle di Posta elettronica

L'AOO si è dotata di una casella di posta elettronica certificata (PEC) istituzionale per la corrispondenza, sia in ingresso che in uscita.

Tutte le UOR che ad essa fanno riferimento sono anch'esse dotate di casella PEC per la corrispondenza sia in entrata che in uscita.

Sono state previste anche caselle PEC per la ricezione delle fatture elettroniche e l'invio degli esiti. La loro gestione completamente automatica prevede l'inserimento nel registro di PG e nel registro delle Fatture nonché nella procedura della contabilità.

Sistema di classificazione dei documenti

Con l'inizio dell'attività operativa del protocollo informatico, è stato adottato un unico Titolario di classificazione per l'archivio centrale unico dell'amministrazione.

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 procedimenti amministrativi.

Formazione

Nell'ambito dei piani formativi richiesti a tutte le pubbliche amministrazioni sulla formazione e la valorizzazione del personale, l'amministrazione stabilisce periodicamente percorsi formativi, specifici e generali, che coinvolgono tutte le figure professionali.

Accreditamento dell'AOO all'IPA

L'AOO, e le UOR che da essa dipendono, come già detto, sono dotate di casella PEC attraverso cui trasmettono e ricevono documenti informatici soggetti alla registrazione di protocollo. Tali caselle sono affidate alla responsabilità delle singole UOR di riferimento, in particolare, la casella istituzionale dell'AOO è gestita dal Protocollo Generale (PG).

Gli incaricati procedono alla lettura della corrispondenza ivi pervenuta entro il primo giorno lavorativo successivo alla ricezione.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), fornendo le informazioni che individuano l'amministrazione e l'articolazione della sua AOO.

Il codice identificativo dell'amministrazione, generato e attribuito autonomamente dall'IPA è CRSA.

Denominazione	Consiglio per la ricerca e l'analisi dell'economia agraria
---------------	---

Codice IPA	CRSA
Acronimo	CREA

Nel registro è stato definito il seguente Elenco uffici:

NOME	SEDE
Amministrazione centrale	Via della Navicella 2-4 - 00184 Roma (RM)
Centro di ricerca Agricoltura e Ambiente	Via della Navicella 2-4 - 00184 Roma (RM)
Centro di ricerca Alimenti e Nutrizione	Via Ardeatina 546 - 00178 Roma (RM)
Centro di ricerca Cerealicoltura e Colture Industriali	S.S. 16 km 675 - 71122 Foggia (FG)
Centro di ricerca Difesa e Certificazione	Via C. G. Bertero 22 - 00156 Roma (RM)
Centro di ricerca Foreste e Legno	Viale Santa Margherita 80 - 52100 Arezzo (AR)
Centro di ricerca Genomica e Bioinformatica	Via San Protaso 302 - 29017 Fiorenzuola d'Arda (PC)
Centro di ricerca Ingegneria e Trasformazioni agroalimentari	Via della Pascolare 16 - 00015 Monterotondo (RM)
Centro di ricerca Olivicoltura, frutticoltura e agrumicoltura	Contrada Li Rocchi Vermicelli 83 - 87036 Rende (CS)
Centro di ricerca Orticoltura e Florovivaismo	Via Cavallegeri 25 - 84098 Pontecagnano Faiano (SA)
Centro di ricerca Politiche e Bioeconomia	Via Barberini 36 - 00187 (RM)
Centro di ricerca Viticoltura ed Enologia	Via XXVIII Aprile 26 - 31015 Conegliano (TV)
Centro di ricerca Zootecnia e Acquacoltura	Viale Piacenza 29 - 26900 Lodi (LO)
Ufficio per la transizione al Digitale	Via della Navicella 2-4 - 00184 Roma (RM)

L'IPA è accessibile, tramite il relativo sito internet, a tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità dell'indirizzo di posta elettronica indicato. Con la stessa tempestività, l'amministrazione comunica la creazione, ovvero la soppressione di una AOO.

Dematerializzazione dei procedimenti amministrativi della AOO

L'amministrazione sta realizzando procedure che consentano, in coerenza con le disposizioni normative e regolamentari in materia, la produzione, gestione, invio e conservazione di documenti amministrativi digitali.

È prevista la riproduzione su carta degli originali digitali, firmati e protocollati, solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti digitali.

Gli eventuali documenti cartacei ricevuti, dopo registrazione e segnatura di protocollo, sono sottoposti al processo di scansione per la loro archiviazione digitale; la UOR destinataria dovrà conservare gli originali cartacei secondo i termini di legge.

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

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei registri di protocollo diversi dal protocollo informatico.

Piano di attuazione

In coerenza con quanto previsto e disciplinato dal presente manuale, tutti i documenti inviati e ricevuti dalla AOO sono registrati nel registro ufficiale di protocollo informatico. Pertanto, tutti gli eventuali registri di protocollo, interni alle UOR e/o agli UU, diversi dal registro ufficiale di protocollo informatico, sono aboliti ed eliminati.

Fa eccezione il registro di repertorio delle fatture elettroniche della PA.

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, anche in relazione alle norme sulla protezione dei dati personali.

Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- i dati personali vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato 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.

Generalità

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore dei servizi cloud per il SdP. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

Il piano di sicurezza:

- si articola in due componenti: una di competenza del SdP, una di competenza della AOO;
- definisce:
 - a. le politiche generali e particolari di sicurezza da adottare all'interno, rispettivamente, dell'erogatore di servizi cloud e della AOO;
 - b. le modalità di accesso al SdP;
 - c. le misure tecniche e organizzative adeguate, così come previsto dall'art.32 del Regolamento.
 - d. i piani specifici di formazione degli addetti;

- e. le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi.

I dati personali registrati nel *log* del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

Misure di sicurezza

Il Responsabile dei Sistemi informativi, al fine di assicurare la sicurezza dell'impianto tecnologico del CREA, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, adotta le misure tecniche e organizzative di seguito specificate:

- autenticazione al sistema mediante SSO (Single Sign-On) reso disponibile tramite protocollo LDAP che permette agli utenti di accedere a più applicazioni e servizi con un'unica password;
- cambio delle password con frequenza almeno trimestrale;
- protezione della rete dell'Amministrazione con sistemi WAF (Web Application Firewall);
- memorizzazione dei log all'interno delle Virtual Machine dove è presente l'applicativo.

Abilitazioni all'utilizzo delle funzionalità del prodotto di protocollo informatico

Il software applicativo utilizzato in rete permette di gestire diversi livelli di accesso agli archivi informatizzati.

I livelli di autorizzazione per l'accesso alle funzioni della procedura informatica di gestione documentale vengono rilasciati dalla competente struttura centrale che gestisce le risorse tecnologiche, previa autorizzazione del Responsabile della Gestione Documentale e su indicazione dell'Ufficio del Personale e sui Titolari dei singoli uffici (Utente TIT). I livelli di autorizzazione si distinguono tra abilitazioni alla consultazione, all'inserimento e alla modifica dei dati registrati.

La gestione delle utenze rispetta i seguenti principi:

- gli utenti creati non sono mai cancellati, ma, eventualmente, disabilitati (su richiesta esplicita del Responsabile della Gestione Documentale);
- la credenziale privata degli utenti non transita in chiaro sulla rete, né al momento della prima generazione, né, successivamente, al momento del login. L'applicativo non tiene traccia delle password degli utenti in quanto l'autenticazione avviene su LDAP, il protocollo utilizzato per accedere all'applicativo è HTTPS.

Le utenze possono avere i seguenti ruoli:

- Amministratore Piattaforma: tipologia in carico al responsabile ICT e al fornitore applicativo, permette di gestire e configurare il prodotto;
- Gestione personale: consente di creare nuove anagrafiche dipendenti, modificare le assegnazioni agli uffici, gestire trasferimenti interni e registrare le cessazioni del rapporto di lavoro;

- Utenze di servizio: viene utilizzata per le integrazioni tra Documentale e altri applicativi;
- Utenti appartenenti all'ufficio protocollo: tipologia di utenza appartenente al gruppo/ufficio UDG8 - Protocollatori ufficio protocollo generale 101_23_03_PROT, sono abilitate alla protocollazione della PEC istituzionale;
- Ruolo Protocollatore Ufficio: gli utenti assegnati a questo ruolo hanno la possibilità di effettuare la protocollazione dei documenti, è previsto almeno un protocollatore per ciascun ufficio. Per i ruoli definiti nella sezione Amministrazione delle mailbox (PEC), oltre alla protocollazione dei documenti creati, gli utenti possono anche:
 - a. visualizzare la posta elettronica certificata associata,
 - b. procedere alla protocollazione delle relativa PEC.
- Ruolo Responsabile di Protocollo: gli utenti appartenenti a questo ruolo hanno la facoltà di approvare o respingere le richieste di annullamento di protocollo.
- Utente TIT: hanno la responsabilità di decidere le variazioni relative ai ruoli e al personale all'interno del proprio ufficio, le decisioni vengono comunicate agli utenti appartenenti al Ruolo Gestione Personale, i quali provvedono ad aggiornare il sistema documentale;
- Utente semplice: Tutti gli altri utenti (attualmente più di 2000) sono definiti come utenti semplici. Essi utilizzano il sistema documentale/protocollo per le attività operative, tra cui:
 - a. creazione di documenti,
 - b. assegnazioni,
 - c. fascicolazione,
 - d. classificazione,
 - e. altre funzioni di base.

Riservatezza dei documenti di Protocollo

La visibilità dei documenti di protocollo è assegnata per gruppi all'interno di un Ufficio specifico associato all'utente. In generale, gli utenti possono vedere i documenti all'interno del loro ruolo e del loro Ufficio di appartenenza sia per la fase di invio che per quella di ricezione del documento. Infatti, un documento di protocollo interno inviato da un protocollatore di un ufficio mittente verso un ufficio destinazione è visibile a tutti i membri dei gruppi "ufficio mittente" e "ufficio destinazione" oltre a coloro i quali svolgono attività di supervisione complessiva delle funzionalità del sistema (es. Responsabile del sistema di gestione di protocollo e Vicario). Tuttavia, in alcuni casi, di seguito elencati, è emersa la necessità di aumentare la riservatezza finalizzata a tutelare la sfera privata dei soggetti presenti nella documentazione inviata e acquisita dagli uffici:

- Flusso Provvedimenti Disciplinari: Solo gli utenti con il ruolo Direttore potranno avviare la creazione di un'unità documentaria di tipo "Provvedimento disciplinare". I documenti protocollati hanno diritti di accesso limitati a: Direttore (mittente), Ufficio Provvedimenti Disciplinari (destinatario), Responsabile di protocollo.
- Flusso Avvocatura: Solo gli utenti appartenenti all'ufficio legale (o ad un determinato ruolo dell'ufficio) potranno avviare la creazione di un'unità documentaria di tipo "Avvocatura". I documenti protocollati hanno diritti di accesso limitati a: Ufficio legale (mittente), utente destinatario e responsabile di protocollo.

- Flusso Whistleblowing: Solo gli utenti appartenenti all'ufficio Whistleblowing (o ad un determinato ruolo dell'ufficio) potranno avviare la creazione di un'unità documentaria di tipo "Whistleblowing". I documenti protocollati devono avere diritti di accesso limitati all'ufficio Whistleblowing.

Backup Sistema

L'applicativo che espleta il servizio di Protocollo risiede all'interno dell'infrastruttura Cloud del PSN (Polo Strategico Nazionale). Allo stato attuale è previsto il Backup mediante snapshot della Virtual Machine (VM), caratterizzato dai seguenti parametri:

- RTO (Recovery Time Objective): 24 ore;
- Frequenza full: settimanale;
- Frequenza differenziale: 24 ore;
- Retention: 30 giorni.

Formazione dei documenti – Aspetti attinenti alla sicurezza

Il documento informatico, identificato in modo univoco e persistente, è memorizzato nel sistema di documentale della AOO che ne garantisce l'inalterabilità, la riservatezza e la fruibilità da parte di persone dotate di adeguate autorizzazioni.

L'evidenza informatica corrispondente al documento informatico imm modificabile è prodotta in uno dei formati contenuti nell'allegato 2 delle Linee Guida Agid, in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità.

Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo del *server* che ospita i *file* utilizzati come deposito dei documenti è configurato in maniera da consentire:

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

Il sistema di gestione documentale:

- 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 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 adottato.

Per la gestione dei documenti informatici all'interno dell'AOO, il RSP fa riferimento alle norme stabilite dal responsabile dell'Ufficio "Sistemi informativi" del CREA.

Trasmissione ed interscambio dei documenti informatici

Gli addetti delle AOO alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono conoscere il contenuto 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.

Come previsto dalla normativa vigente, 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, 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 l'AOO, oltre alle funzioni di un *server* SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO 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 dal decreto legislativo 10 agosto 2018, n. 101.

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.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (*UserID*) e privata (*Password*) e un sistema di autorizzazioni basato sulla creazione di specifici profili utente.

La creazione di profili utente consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale dell'Ente. Queste sono le abilitazioni/autorizzazioni previste:

- *Consultazione* – consente di visualizzare in modo selettivo le registrazioni di protocollo eseguite da altri;

- *Inserimento* – permette di inserire gli estremi di protocollo, effettuare una registrazione di protocollo e associare documenti;
- *Annullamento* – consente di richiedere l'annullamento di una registrazione di protocollo, previa motivazione esplicita, al RSP.

Le regole per la composizione delle password e il blocco delle utenze valgono sia per l'amministratore che per gli utenti della AOO.

Le relative politiche di composizione, aggiornamento e, in generale, di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

Il sistema di protocollo, così come la gestione documentale seguono la logica dell'organizzazione dell'Ente, pertanto ciascun utente può accedere solamente ai documenti che sono assegnati alla sua UOR o ai GO ad essa subordinati.

La piattaforma:

- 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 da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una *Access Control List (ACL)* che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale dell'archivio o di una ricerca *full text*.

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal CGD dell'AOO, sentito il RSP.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita del Titolare UOR o per errori di inserimento);
- le credenziali private degli utenti sono gestite attraverso il sistema di autenticazione Microsoft e non transitano in chiaro sulla rete, né al momento della prima generazione, né successivamente, al momento del login.

Accesso al registro di protocollo per utenti interni alla AOO

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del Sistema di Protocollo" (RSP) e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una visione parziale sul registro di protocollo. Tale visione è definita dalla lista di competenza dei singoli documenti in cui l'utente è presente come UOR/GO di appartenenza.

Utenti esterni alla AOO - Altre AOO/Amministrazioni

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

Utenti esterni alla AOO – Privati

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

Conservazione dei documenti informatici

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie e garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, dei seguenti oggetti digitali:

- a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del TUDA e art. 44, comma 1-bis del CAD;
- c) gli archivi informatici con i metadati associati.

Il registro giornaliero di protocollo è trasmesso, entro la giornata lavorativa successiva, al sistema di conservazione; in questo modo viene garantita l'immodificabilità del contenuto.

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

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per la formazione e lo scambio di documenti all'interno ed all'esterno dell'AOO.

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione, si distinguono in:

- documenti ricevuti (in entrata),
- documenti inviati (in uscita),
- documenti interni (comunicazioni tra UOR senza destinatari esterni).

Per documenti in entrata si intendono tutti i documenti di rilevanza giuridico probatoria acquisiti dal CREA nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Per documenti in uscita si intendono i documenti di rilevanza giuridico probatoria prodotti dall'Ente nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

I documenti interni, prodotti e trasmessi tra le diverse UOR, sono formati con tecnologie informatiche.

Il documento analogico – cartaceo

Il documento analogico è formato utilizzando segni continui riprodotti su un idoneo supporto fisico (ad es. carta), leggibili senza l'ausilio di strumenti tecnologici.

Il documento amministrativo cartaceo può essere prodotto in maniera tradizionale (esempio: lettera scritta a mano o a macchina), oppure con strumenti informatici (esempio: lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampato.

In quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.

Le PA sono obbligate a formare gli originali dei loro documenti come documenti informatici adeguando a tal fine i loro sistemi di gestione documentale così come previsto dall'art. 40 c. 1 del CAD che recita *“Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida”*.

La copia informatica per immagine di documenti analogici è disciplinata dall'art. 22 del CAD, che in particolare, ai commi 1 e 1bis, così recita:

“I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del Codice civile, se sono formati ai sensi dell'articolo 20, comma 1-bis, primo periodo. La loro esibizione e produzione sostituisce quella dell'originale.

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.”

Le copie formate secondo quanto indicato nel CAD sostituiscono a tutti gli effetti gli originali, formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge. Con Decreto del Presidente del Consiglio dei Ministri possono però essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico. In caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

Documenti ricevuti

La corrispondenza in ingresso deve essere acquisita dall'Amministrazione sulla piattaforma di gestione documentale con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

I documenti informatici ricevuti:

- per posta elettronica convenzionale o certificata,
- attraverso un supporto rimovibile quale, ad esempio, cd rom, dvd, floppy disk, tape, pen drive, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere,

sono sottoposti al sistema di registrazione e sono acquisiti nel sistema di gestione documentale, attraverso il quale sono successivamente smistati.

I documenti analogici ricevuti:

- per posta convenzionale o corriere;
- per posta raccomandata;
- *brevi manu* mediante consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata, agli UOR aperti al pubblico,

sono sottoposti al sistema di registrazione, scansione e inserimento nel sistema di gestione documentale, attraverso il quale sono successivamente smistati e conservati a cura della UOP ricevente.

Documenti inviati

Le comunicazioni di documenti tra le PA avvengono mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il documento può essere, altresì, reso disponibile previa comunicazione delle modalità di accesso telematico allo stesso.

I documenti informatici, compresi gli eventuali allegati anch'essi informatici, sono inviati, di norma, per mezzo di interoperabilità di protocollo o posta elettronica certificata.

In alternativa, il documento informatico può essere riversato su supporto rimovibile non modificabile e trasmesso con altri mezzi di trasporto al destinatario.

Documenti interni formali

La trasmissione tra UOR di documenti interni formali avviene attraverso il sistema di gestione documentale.

Il documento interno è registrato nel sistema di gestione documentale come protocollo interno ed è assegnato alla UOR destinataria tramite la funzione di assegnazione; non deve pertanto essere registrato anche dalla UOR di destinazione.

Non è possibile utilizzare la posta elettronica certificata delle UOR per lo scambio di documenti interni formali.

Documenti interni informali

Rientrano in questa categoria le comunicazioni informali tra le diverse UOR appartenenti alla AOO. Tali comunicazioni sono ricevute e trasmesse per mezzo di posta elettronica istituzionale e, di norma, non sono protocollate.

Formazione dei documenti informatici– Aspetti operativi

Il documento informatico è formato mediante una delle seguenti modalità:

- a) redazione tramite l'utilizzo di strumenti software;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il CAD determina quattro caratteristiche oggettive che individuano un documento informatico a norma di legge:

- qualità;
- sicurezza;
- integrità;
- immodificabilità.

Il documento informatico deve essere identificato in modo univoco e persistente ed è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

L'immodificabilità e l'integrità di un documento, qualunque siano le modalità seguite per la sua formazione, sono garantite dall'apposizione di una firma elettronica qualificata, di una firma digitale, di un sigillo elettronico qualificato o di una firma elettronica avanzata.

Nel caso di documento informatico formato secondo le lettere a) e b) le caratteristiche di immodificabilità e di integrità sono garantite anche mediante una o entrambe le operazioni seguenti:

- memorizzazione su sistemi di gestione documentale che adottino idonee misure di protezione;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le lettere c) e d) le caratteristiche di immutabilità e di integrità sono garantite anche mediante una o entrambe le operazioni seguenti:

- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico;
- produzione di un'estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto al documento stesso.

Al momento della formazione del documento informatico immutabile, devono essere generati e associati permanentemente ad esso i relativi metadati.

I metadati sono l'insieme di dati associati ad un documento informatico, o ad un'aggregazione documentaria, per identificarlo, descriverne il contenuto e consentirne la gestione e la conservazione nel tempo.

Formazione dei documenti informatici amministrativi – Aspetti operativi

Si definisce documento amministrativo ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle PA, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa ai sensi dell'art. 22, della Legge 7 agosto 1990, n. 241. Per documento amministrativo informatico si intende, ai sensi dell'art. 23 ter del CAD, l'atto formato dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse.

La PA forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli artt. 5-bis, 40-bis e 65 del CAD che sono identificate e trattate come i documenti amministrativi informatici.

Il documento amministrativo informatico assume le caratteristiche di immutabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1 delle Linee guida Agid, anche con la sua registrazione nel registro di protocollo e negli eventuali registri contenuti nel sistema di gestione documentale con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato un insieme di metadati, come indicato dalle Linee guida e così come previsto dagli artt. 53 e 56 del TUDA, riguardanti, le operazioni di registrazione, di segnatura di protocollo e di classificazione.

Inoltre, sono associati i metadati atti a fornire le informazioni relative alla modalità di formazione e alla tipologia del documento, alla presenza di allegati, alla riservatezza dello stesso, alle informazioni per identificare il formato, alla versione, e, infine, all'esito delle verifiche a cui il documento viene sottoposto.

Fanno eccezione i documenti soggetti a registrazione particolare a cui comunque vengono associati l'insieme dei metadati previsti per il documento informatico immutabile.

Il documento deve essere sottoscritto prima di venire inserito nel sistema di gestione documentale per la protocollazione.

Sottoscrizione dei documenti informatici

La sottoscrizione ha un ruolo centrale nell'assicurare il rispetto dei requisiti previsti per la formazione dei documenti delle PA.

In particolare, contribuisce a garantire:

- la verifica della provenienza;
- l'integrità (nel caso del supporto cartaceo si firma in calce al documento e, in alcuni casi, su ogni pagina);
- la paternità (intesa come assunzione di responsabilità);
- l'autenticità del documento.

Per la sottoscrizione dei documenti informatici si utilizza il sistema della firma elettronica.

Il documento informatico soddisfa pienamente il requisito della forma scritta e ha l'efficacia probatoria, prevista dall'art. 2702 c.c., se sono rispettate le seguenti condizioni:

- è riconducibile all'autore in modo certo: è necessario identificare la persona fisica, ma anche il contenuto sottoscritto come sua manifestazione di volontà;
- il processo di formazione del documento ne garantisce la sicurezza, l'integrità e l'immodificabilità.

L'utilizzo di una firma avanzata, di cui la firma digitale è una fattispecie, soddisfa entrambe le condizioni consentendo la verifica della identità dell'autore e l'integrità dei contenuti del documento.

In assenza di tali condizioni, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, sempre in relazione alle caratteristiche di sicurezza, integrità e immodificabilità del documento medesimo.

Requisiti degli strumenti informatici di scambio

Lo scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi consiste nel garantire l'interoperabilità e il rispetto dei requisiti minimi di sicurezza di seguito elencati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno della AOO;
- l'interconnessione tra UOR;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

Firma digitale e firma elettronica

La firma elettronica è il risultato di una procedura informatica che consente (in forme e gradi diversi, in base alla tecnologia e al modello utilizzati) di rendere manifesta l'autenticità del documento informatico (e la sua capacità di prova) e di verificarne la provenienza e l'integrità.

Il legislatore europeo ha individuato diversi tipi di firma elettronica: semplice (FE), avanzata (FEA), qualificata (FEQ).

La firma elettronica senza ulteriori attributi è definita nel Regolamento eIDAS come *“l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica”*.

La firma elettronica semplice (detta firma debole) ha una efficacia probatoria limitata in quanto non garantisce né l'integrità né l'identificazione univoca e manifesta del firmatario; per questi motivi è liberamente valutabile dal giudice in base all'analisi delle sue caratteristiche oggettive di qualità e sicurezza.

Le firme elettroniche avanzate e qualificate:

- sono basate su un certificato che identifica il firmatario in modo manifesto e univoco;
- sono create mediante un dispositivo sicuro di cui il firmatario ha il pieno controllo;
- collegano la firma ai dati cui si riferisce in modo da consentire l'identificazione di ogni loro successiva modifica.

Il certificato qualificato è un documento elettronico rilasciato da enti terzi, denominati prestatori di servizi fiduciari qualificati, e finalizzato a identificare con certezza il titolare di una firma elettronica qualificata (identità e chiave pubblica). In particolare, è un file generato seguendo precise indicazioni e standard stabiliti per legge e al suo interno sono conservate informazioni che riguardano:

- l'identità del titolare;
- la chiave pubblica attribuitagli al momento del rilascio;
- il periodo di validità del certificato stesso;
- i dati dell'ente certificatore.

Nel certificato digitale possono essere inserite una serie di informazioni ulteriori riguardanti il sottoscrittore: per esempio il titolo, le limitazioni d'uso, le limitazioni nei valori negoziali, l'utilizzo di sottoscrizione con procedura automatica.

La firma elettronica avanzata è definita come insieme di dati in forma elettronica allegati oppure connessi a un documento informatico in grado di identificare in modo univoco il firmatario del documento e creati con mezzi sui quali il firmatario può conservare un controllo esclusivo e rilevare se i dati stessi siano stati successivamente modificati.

Garantisce integrità, autenticità del documento sottoscritto e controllo esclusivo dello strumento di firma. Non ha valenza generale, in quanto legata a un accordo tra le parti. Non è quindi adatta ai documenti delle PA con valenza esterna e generale.

La firma elettronica qualificata è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

La firma elettronica qualificata è associata stabilmente al documento informatico sulla quale è apposta e include informazioni che ne attestano con certezza l'integrità, l'autenticità, la non ripudiabilità, consentendo al documento così sottoscritto di assumere la piena efficacia probatoria.

I dispositivi devono garantire la conformità a requisiti di sicurezza molto stringenti fissati dalla normativa vigente, per assicurare il controllo esclusivo del firmatario sulla propria firma.

Il dispositivo di firma elettronica qualificata si presume riconducibile al titolare della firma, salvo che questi fornisca prova contraria in modo concreto e inequivocabile.

La firma digitale è un particolare tipo di firma elettronica qualificata basato su un certificato qualificato e su dispositivo sicuro, costituito da un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici indipendentemente dal tipo di supporto fisico sul quale è memorizzato. È rilasciata da prestatori qualificati di servizi fiduciari che forniscono, ai titolari di firma, certificati qualificati attestanti l'identità del titolare della coppia di chiavi.

Per ragioni di sicurezza relative al rischio di violabilità, la firma digitale ha una validità limitata nel tempo (tre anni in Italia). Il dispositivo di firma utilizzato deve essere dotato di un certificato qualificato che, al momento della sottoscrizione, non deve risultare scaduto, revocato o sospeso.

Nessuna firma elettronica costituisce riferimento temporale. La validazione temporale di un documento informatico è il risultato della procedura informatica con cui si attribuiscono, a uno o più documenti informatici, una data ed un orario opponibili ai terzi, cioè verificabili *erga omnes*.

La normativa italiana prevede quattro tipologie di riferimento temporale in grado di assicurare la validazione temporale (in quanto capacità di disporre di un riferimento temporale opponibile a terzi) dei documenti informatici:

- il riferimento temporale incluso nella segnatura di protocollo delle pubbliche amministrazioni;
- il riferimento temporale ottenuto attraverso il processo di conservazione dei documenti, a opera di un pubblico ufficiale o di una PA o di un conservatore accreditato;
- il riferimento temporale ottenuto attraverso l'utilizzo di PEC;
- il riferimento temporale ottenuto attraverso la marca elettronica.

Verifica delle firme SdP per i formati .p7m

Nel SdP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati. La sequenza delle operazioni previste è la seguente:

- apertura della busta «virtuale» contenente il documento firmato;
- verifica della firma (o delle firme multiple);
- verifica della validità del certificato;
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica.

Uso posta elettronica certificata

La Posta Elettronica Certificata (PEC) ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale.

L'utilizzo della 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.

La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso con PEC e redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi.

Ogni PA ha l'obbligo di creare una casella PEC per ogni registro di protocollo e comunicare ciascun indirizzo all'Agid.

Ciascuna UOR in cui è articolata la AOO ha una PEC che deve essere utilizzata unicamente per comunicare con AOO o UOR esterne al CREA. Non è consentito l'uso della PEC per comunicazioni tra le UOR del CREA.

Anche il CAD fa esplicito riferimento alla posta elettronica certificata agli artt. 6 e 48.

L'art. 6, comma 1, sancisce che *“per le comunicazioni di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano”*.

L'art. 48, comma 1 prevede che *“la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con le regole tecniche adottate ai sensi dell'articolo 71”*.

Al comma 2 viene sancito che *“la trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta”*.

Al comma 3 si precisa che *“la data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche. Il Codice dell'Amministrazione Digitale fa esplicito riferimento alla posta elettronica certificata agli artt. 6 e 48”*.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

L'Ufficio di protocollo non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai documenti che possono avere rilevanza giuridico probatoria.

Essi si riferiscono ai documenti:

- ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;
- inviati dalla AOO all'esterno;
- interni formali prodotti e scambiati all'interno della AOO.

Le comunicazioni informali tra uffici intese come scambio di informazioni, con o senza allegati, delle quali è facoltativa la conservazione non interessano il sistema di protocollo.

Un documento si definisce:

- in entrata se il mittente è esterno;
- in uscita se è presente almeno un destinatario esterno. In caso di destinatari interni ed esterni, i destinatari interni ricevono esclusivamente l'assegnazione del documento;
- interno se tutti i destinatari sono UOR dell'Ente. I documenti in uscita e/o interni devono essere a firma del Titolare UOR (Dirigente dell'Ufficio o Direttore del Centro di ricerca).

Flusso dei documenti in ingresso alla AOO

I documenti informatici in arrivo sono accessibili al personale specificatamente individuato che giornalmente provvede ad aprire, leggere, registrare, segnare, smistare, classificare ed assegnare agli uffici competenti i documenti pervenuti. L'informativa della registrazione è resa disponibile attraverso un **messaggio di notifica** che l'operatore di protocollo può inviare all'indirizzo di posta elettronica assegnataria.

I documenti pervenuti dai dipendenti dell'Ente vengono acquisiti nel protocollo in entrata.

I documenti ricevuti da più UOR devono essere protocollati dalla UOR destinataria principale che li assegnerà alle UOR in copia al messaggio. Queste ultime scartano il messaggio di posta con motivazione **Messaggio protocollato dal destinatario principale specificando eventualmente il numero di protocollo**.

Il documento informatico che perviene nella casella di PEC va gestito, di norma, entro le 24 ore lavorative successive alla ricezione. Comunque, data ed orario di ricezione della PEC sono resi visibili dal sistema. La registrazione in entrata via PEC non permette di modificare i file informatici associati ad essa.

Se il documento informatico allegato alla PEC è privo di firma, durante la protocollazione, va evidenziato nel campo "Note" la dicitura *Documento non firmato*. Qualora il documento ricevuto non

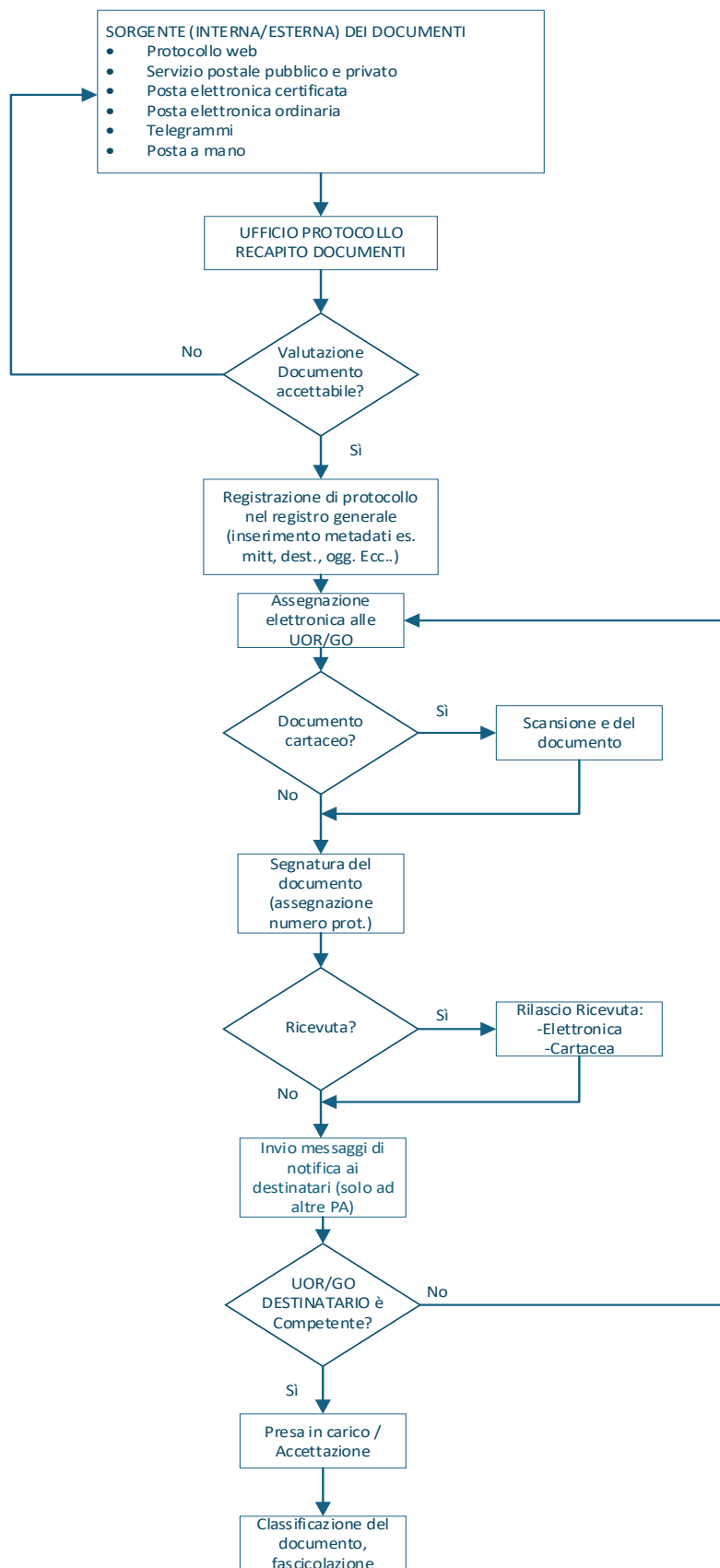
sia pdf o pdf/a (con o senza firma digitale) viene comunque registrato al protocollo. Spetta al Responsabile del procedimento valutare se accettare il documento informatico assegnato non sottoscritto o non conforme agli standard.

Procedure per la gestione dei documenti in entrata (flow chart)

La documentazione pervenuta viene registrata e protocollata nel medesimo giorno in cui è stata ricevuta.

Le fasi della gestione dei **documenti in entrata** (interni alla stessa AOO, sia da altre Amministrazioni o da esterni Privati) sono elencate nei seguenti punti e debbono essere effettuate rigorosamente nell'ordine indicato:

- a) **ricezione;**
- b) **registrazione nel sistema di protocollo e segnatrice** di protocollo che riporta le principali informazioni riguardanti il documento registrato: AOO di appartenenza, numero di protocollo, data di registrazione (la segnatrice manuale vale per documenti cartacei);
- c) **assegnazione:** attribuzione del documento all'Unità Organizzativa Responsabile (UOR) competente per il relativo procedimento e contestuale assegnazione al Responsabile dell'UOR o ad altra persona da questi indicata;
- d) eventuale **scansione** ove si tratti di documenti su supporto cartaceo;
- e) eventuale rilascio della **ricevuta;**
- f) **classificazione** (rif. Titolario o Piano di Classificazione);
- g) **fascicolazione** (rif. Fascicoli o Dossier).



Flusso dei documenti in uscita dalla AOO

Per "documenti in uscita" s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione, ovvero ad altro ufficio (UOR) della stessa AOO.

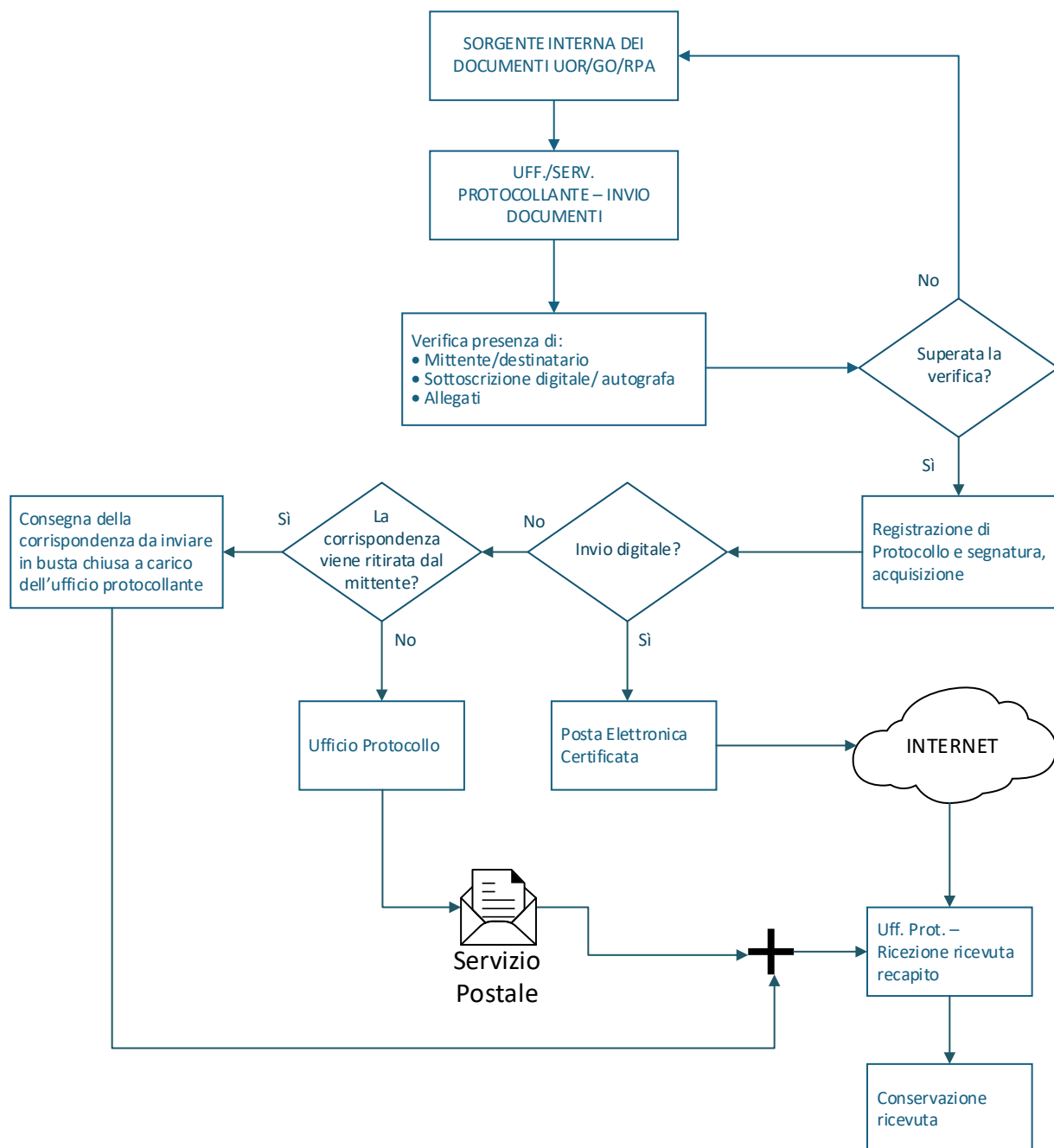
Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di PEC, conforme a quanto previsto dal DPR 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

Procedure per la gestione dei documenti in uscita (flow chart)

Le fasi della gestione dei documenti in uscita (all'interno della stessa AOO ad altre Amministrazioni o da corrispondenti Privati) sono elencate nei seguenti punti e debbono essere effettuate rigorosamente nell'ordine indicato:

- a) produzione;
- b) acquisizione del documento e/o del file del documento informatico;
- c) registrazione nel sistema di protocollo: indicazione della UOR/GO /RPA mittente del documento ed indicazione di altri eventuali funzionari dell'AOO destinatari di copia per conoscenza del documento, cui perviene la notifica automatica;
- d) apposizione della segnatura di protocollo (la segnatura manuale vale per documenti cartacei);
- e) eventuale scansione del documento e dei suoi allegati nel caso in cui siano su supporto cartaceo;
- f) classificazione;
- g) fascicolazione;
- h) spedizione per protocollo web, pec, posta ordinaria, fax, raccomandata, assicurata, etc.. Se posta ordinaria, fax, raccomandata, assicurata la spedizione avverrà tramite l'Ufficio Protocollo;
- i) archiviazione della copia del documento nell'archivio dell'UOR/GO/RPA mittente.

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.



6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

Regole disponibili con il SdP

Lo smistamento e l'assegnazione dei documenti avviene in base al modello delle competenze, così come definito nella struttura organizzativa dell'Ente.

Attività di assegnazione

L'attività di assegnazione effettuata dalla UOP consiste nell'operazione di inviare direttamente all'UOR competente il documento protocollato e segnato e nella contestuale trasmissione del materiale documentario oggetto di trattazione.

Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel RPA designato.

Preso atto dell'assegnazione, il RPA verifica la competenza e provvede alla presa in carico del documento che gli è stato assegnato.

L'UOR competente è incaricata della gestione del procedimento cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che si avvia con l'assegnazione del documento decorrono comunque dalla data di protocollazione.

Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è inviato in busta chiusa direttamente al Direttore generale.

Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione e segnatura di protocollo.

L'UOR competente ha notizia dell'assegnazione di detti documenti tramite l'incremento del numero (badge) delle *Attività in entrata* da prendere in carico sul sistema di gestione documentale.

Assegnazione dei documenti ricevuti in formato cartaceo

Al termine delle operazioni di registrazione e segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati alla UOR di appartenenza dell'RPA sul sistema di gestione documentale.

L'originale cartaceo viene trattato come di seguito indicato:

- viene acquisito in formato PDF/A con l'ausilio di scanner;
- può essere successivamente trasmesso/ritirato al/dal RPA, oppure essere conservato dalla UOP.

I documenti cartacei gestiti dalla UOP sono di norma assegnati entro il giorno lavorativo successivo a quello di ricezione. L'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo alla ricezione.

Come per i documenti digitali, l'UOR competente ha notizia dell'arrivo/assegnazione del documento ad esso indirizzato tramite il badge sulle attività in entrata del sistema documentale.

Attraverso le funzioni del SdP e in base alle abilitazioni previste il responsabile dell'UOR potrà:

- visualizzare gli estremi del documento ed il contenuto;
- individuare come assegnatario il RPA competente nella materia oggetto del documento.

La "presa in carico" dei documenti informatici è registrata dal sistema in modo automatico e la data di ingresso dei documenti nelle UOR di competenza coincide con la data di assegnazione degli stessi.

Modifica delle assegnazioni

Nel caso di smistamento o assegnazione errati, l'Ufficio che riceve il documento provvede ad effettuare il "rifiuto" del documento tramite il sistema gestionale. Ciò consente all'Ufficio mittente di procedere ad un nuovo smistamento o assegnazione e all'errato destinatario di non mantenere i privilegi di visione e conoscenza che gli sono stati erroneamente attribuiti. Qualora il documento sia stato trasmesso anche in formato cartaceo, lo stesso deve essere restituito all'Ufficio che lo ha inviato. In un'ottica di celerità e semplificazione l'Ufficio che riceve per errore un documento non di propria pertinenza ma destinato ad altro soggetto della propria UOR, potrà inoltrarlo direttamente all'Ufficio competente, eventualmente segnalando l'errore al mittente. I termini per la definizione del procedimento amministrativo che eventualmente prende avvio dal documento decorrono comunque dalla data di protocollazione.

7. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI

Il presente capitolo riporta le regole di gestione dei documenti in uscita adottate dalla UOP.

L'UOP dopo aver protocollato in uscita il documento lo assegna all'Ufficio proponente. Tale assegnazione è generata automaticamente dal SdP ed è la conferma dell'avvenuta protocollazione del documento.

In caso di destinatari interni su documenti in uscita (indirizzati ad almeno un destinatario esterno), il documento deve essere assegnato alla UOR competente.

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

Documenti esclusi

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del TUDA, di seguito riportati:

- a) gazzette ufficiali;

- b) bollettini ufficiali;
- c) notiziari della pubblica amministrazione;
- d) note di ricezione delle circolari e altre disposizioni;
- e) materiali statistici;
- f) atti preparatori interni;
- g) giornali e riviste;
- h) libri;
- i) materiali pubblicitari;
- j) inviti a manifestazioni che non danno adito all'attivazione di un procedimento amministrativo;
- k) tutti i documenti già soggetti a registrazione particolare dell'amministrazione (cfr. par. 8.2).

Inoltre, sono esclusi dalla registrazione di protocollo tutti documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente e futura, gli atti interni che non costituiscono fasi obbligatorie e imprescindibili dei procedimenti amministrativi, quelli di preminente carattere informativo nonché i documenti di interesse effimero.

Documenti soggetti a registrazione particolare

Sono soggetti a registrazione particolare le fatture elettroniche della PA.

La registrazione particolare consente comunque di eseguire tutte le operazioni previste nell'ambito della gestione documentale, in particolare la classificazione e la fascicolazione.

9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

Protezione e conservazione degli archivi pubblici

Il presente capitolo descrive il sistema di classificazione dei documenti, di formazione del fascicolo e di archiviazione dei documenti, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare la loro corretta organizzazione nell'archivio, è obbligatoria per legge e si avvale del Piano di classificazione, o titolario. Il titolario è definito come un "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

L'archivio è il complesso dei documenti prodotti o comunque acquisiti da una persona fisica o giuridica durante lo svolgimento della propria attività.

Dal punto di vista archivistico si distinguono tre fasi di gestione dei documenti che tengono conto delle diverse modalità di organizzazione e di utilizzo degli stessi:

- archivio corrente: contiene i documenti relativi ad affari, ad attività e a procedimenti amministrativi in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito;
- archivio di deposito: contiene i documenti ancora utili per finalità amministrative o giuridiche ma non più indispensabili per lo svolgimento delle attività correnti;

- archivio storico: contiene documenti storici selezionati per la conservazione permanente. Si tratta del complesso dei documenti per i quali è previsto un tempo di conservazione illimitato che abbiano maturato quarant'anni, fatti salvi i maggiori termini previsti dalla legge.

I singoli documenti di una PA sono beni culturali e quindi sono inalienabili sin dal momento del loro inserimento nell'archivio dell'amministrazione che avviene di norma 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 competente Soprintendenza archivistica. L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta Soprintendenza. Lo scarto dei documenti dell'archivio è subordinato all'autorizzazione di quest'ultima, su proposta del Responsabile della Gestione Documentale (RSP). Il CAD, art. 44, comma 1-bis, stabilisce che, almeno una volta all'anno, il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi.

I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.

Nelle PA, il sistema di gestione documentale trasferisce al sistema di conservazione:

- a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
- b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati:

- i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati.

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali; se sottoposti a scarto devono essere distrutti anche in tutti i sistemi gestiti dal Titolare dell'oggetto di conservazione.

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.

Titolario o piano di classificazione

Il titolario o piano di classificazione è un sistema logico di partizioni astratte (categorie, classi e sottoclassi), gerarchicamente ordinate (dal generale al particolare), definite sulla base delle funzioni e delle attività svolte dall'Amministrazione. Il titolario organizza i documenti secondo una struttura ad albero, raggruppando, in maniera omogenea e coerente, i documenti che si riferiscono alle medesime attività, affari o procedimenti amministrativi.

L'obiettivo del piano di classificazione è:

- descrivere le attività svolte nell'ente secondo un'articolazione logica razionale;
- definire il modo in cui si organizza fisicamente e/o logicamente la documentazione, cioè descrivere tipologie specifiche di fascicoli per ciascuna funzione o macro-attività.

In linea di massima le partizioni corrispondono ai seguenti livelli:

- I livello – Categorie: Funzioni / Materie;
- II livello – Classi: Macro-attività o macro-processi;
- III livello – Sottoclassi: Attività specifiche.

Il piano di classificazione non coincide con l'organigramma (classificazione organica), ma si basa sulle funzioni e sulle materie di competenza dell'Ente (classificazione funzionale).

Attraverso il titolario è possibile definire un quadro alfanumerico di riferimento per l'archiviazione, la conservazione e l'individuazione dei documenti.

Per supportare adeguatamente la creazione ordinata e funzionale dei fascicoli è opportuno che il piano di classificazione sia integrato da indicazioni che riguardano:

- la modalità di formazione dei fascicoli;
- i tempi e le modalità di conservazione;
- le responsabilità per la gestione documentaria;
- il tipo di accesso e il controllo dei diritti connessi all'uso dei documenti.

Il piano di classificazione del CREA (prima CRA) è stato approvato con Decreto del Direttore generale n. 109 del 20 dicembre 2012 (Allegato 1).

Fascicoli e Dossier

Il fascicolo è l'unità di base di un archivio. Ogni fascicolo contiene documenti che si riferiscono a uno stesso affare, attività o procedimento; i fascicoli sono classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal piano di classificazione. Formare fascicoli o fascicolare è l'attività finalizzata ad attribuire ogni documento a un raggruppamento organico coerente rispetto allo svolgimento delle attività dell'ente; le relazioni che si stabiliscono tra i documenti sono rilevanti sul piano giuridico e garantiscono che il legame tra i documenti (il vincolo archivistico) sia ben formato e possa essere mantenuto nel tempo.

I fascicoli sono formati sulla base del piano di classificazione.

Nella progettazione dei fascicoli è necessario evitare:

- la frammentazione o la moltiplicazione non necessarie (non garantiscono la completezza della pratica);
- l'accorpamento eccessivo di documenti all'interno della stessa unità;
- la tendenza a costituire fascicoli intestati ai destinatari. I fascicoli devono infatti fare riferimento al tipo di attività.

Tutti i documenti inviati, ricevuti o interni devono essere fascicolati, indipendentemente dal supporto sul quale sono formati. Eventuali documenti non protocollati ma attinenti alla pratica, vanno inseriti nel fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione (cioè titolo, classe, sottoclasse);
- numero del fascicolo (assegnato automaticamente al momento dell'apertura);
- oggetto del fascicolo, inteso come stringa di testo che descrive compiutamente il contenuto del fascicolo (descrizione);
- lo stato del fascicolo (aperto/chiuso);
- data di apertura del fascicolo (assegnata automaticamente al momento dell'apertura);
- data di chiusura del fascicolo (assegnata automaticamente al momento della chiusura);
- livello di riservatezza (riservato/non riservato e diritti di accesso associati).

I criteri di visibilità dei fascicoli digitali, e degli eventuali loro sottofascicoli all'interno dell'AOO, sono definiti dai vari Responsabili dei Procedimenti Amministrativi.

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, l'addetto al protocollo, con l'eventuale supporto del responsabile del procedimento assegnatario del documento stesso, provvederà all'apertura (istruzione) di un nuovo fascicolo.

Il fascicolo:

- può essere chiuso periodicamente (per esempio su base annuale nel caso di un fascicolo di attività); esempio: il fascicolo "Statistiche delle richieste di accesso";
- può essere chiuso in relazione alla conclusione del procedimento (fascicolo procedimentale) o dell'affare (fascicolo di affare), esempio: il fascicolo relativo a un concorso (fascicolo procedimentale) o il fascicolo relativo a un gruppo di lavoro (fascicolo di affare);
- può avere natura permanente, esempio: i fascicoli del personale o di fornitori che hanno periodici rapporti con l'ente.

Il fascicolo deve essere chiuso esplicitamente, accedendo in modifica sul fascicolo stesso.

Per i documenti di tipo Decreti ed Atti e Delibere è stata predisposta un'apposita gestione che ne prevede il raggruppamento in determinati fascicoli e il relativo invio nel Sistema di Conservazione a Norma all'inizio dell'annualità successiva (entro il mese di gennaio). Il vicario procede all'apertura dei fascicoli per le nuove annualità e alla chiusura dei fascicoli con anzianità maggiore di tre anni.

I documenti sono archiviati all'interno di ciascun fascicolo e/o sottofascicolo, secondo l'ordine cronologico di registrazione nel fascicolo stesso in modo tale che si possa individuare rapidamente il documento inserito più recente.

Il fascicolo si può formare secondo criteri diversi:

- criteri funzionali: tutti i documenti hanno le stesse finalità amministrative ed hanno lo stesso indice di classificazione. Esempi: fascicolo procedimentale, per affare e per attività;
- criteri non funzionali: i documenti contenuti nella stessa aggregazione possono fare riferimento a procedimenti ed affari diversi. Esempi: fascicolo di persona fisica e giuridica.

Sulla base del criterio selezionato avremo le seguenti tipologie di fascicolo:

- **fascicolo per procedimento o per affare.** Il fascicolo si costituisce mediante l'inclusione di tutti i documenti relativi ad un determinato procedimento o affare. Per procedimento si intende una serie di atti formalmente coordinati tra loro rivolti al conseguimento di uno stesso fine; per procedimento amministrativo si intende una serie di atti e di attività finalizzati all'adozione di un provvedimento amministrativo che rappresenta l'atto finale e coincide con la decisione adottata dalla PA che incide direttamente sui diritti e sugli interessi degli amministrati ed è impugnabile dinanzi al giudice. Nel caso dell'affare non è prevista l'adozione di un provvedimento finale né esistono fasi e principi formalmente definiti. Esempi:
 - Concorso a tempo indeterminato per funzionari di amministrazione (fascicolo procedimentale),
 - Gruppo di lavoro sul manuale di gestione documentale (fascicolo per affare);
- **fascicolo per attività.** Il fascicolo conserva i documenti relativi a una competenza procedimentalizzata, per la quale esistono documenti vincolanti o attività di aggiornamento e per la quale non è comunque prevista l'adozione di un provvedimento finale. Questi fascicoli hanno un tempo certo per la chiusura, hanno un contenuto tipico, sono reiterabili nel tempo (ad esempio ogni anno). Esempio: Statistiche sulle richieste di accesso al sito.
- **iperfascicolo o dossier.** L'iperfascicolo include documenti riferiti a più procedimenti e affari. I documenti contenuti non necessariamente devono condividere lo stesso indice di classificazione. L'iperfascicolo risponde ad esigenze di aggregazione di natura funzionale che sarebbero difficilmente gestite in ambiente analogico. Il fascicolo di persona, fisica o giuridica, è un iperfascicolo o dossier. Si tratta infatti di un fascicolo multi-affare, multi-attività e multi-procedimentale. Il fascicolo di persona contiene tutti i documenti utili a ricostruire gli eventi giuridici, organizzativi ed economici relativi a una persona che intrattiene, o ha intrattenuto, rapporti di lavoro con il soggetto produttore. Include documenti relativi a nomina in servizio (procedimento amministrativo), comunicazione della variazione di residenza (attività), assegnazione di un incarico (affare), richiesta di quiescenza (procedimento amministrativo). Mentre il fascicolo procedimentale conserva il complesso dei documenti prodotti, dal primo con il quale il fascicolo è stato istruito e il procedimento avviato, fino al provvedimento finale, il fascicolo di persona può conservare, di un determinato procedimento amministrativo, solo un documento, anche in forma di copia semplice (di norma il provvedimento finale).

Fascicoli del personale

Il fascicolo del personale viene indentificato dai seguenti elementi:

- 3.03.01. COGNOME Nome – CODICEFISCALE. (personale di ruolo)
- 3.03.02. COGNOME Nome – CODICEFISCALE. (personale non di ruolo)

Il fascicolo viene aperto al momento dell'assunzione.

Se una persona passa da tempo determinato – classificazione 3.03.02 – a tempo indeterminato – classificazione 3.03.01 – si chiude il fascicolo e si riapre utilizzando la voce corrispondente del piano di classificazione con la nuova classifica.

I certificati di malattia sono inviati dai medici in forma telematica all'INPS e restano disponibili nella banca dati dell'INPS per l'acquisizione da parte dell'Ente. I certificati di malattia digitali sono una

tipologia di documenti esclusa dalla protocollazione. Eventuali certificati relativi a visite specialistiche rilasciati in forma cartacea potranno essere caricati sui giustificativi di assenza del sistema di rilevazione presenze.

Consultazione e movimentazioni dell'archivio corrente, di deposito e storico

I documenti di una PA sono beni culturali, e quindi inalienabili, sin dal momento del loro inserimento nel sistema di gestione documentale che rappresenta l'archivio corrente.

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 competente Soprintendenza archivistica.

L'archivio corrente è l'insieme organico dei documenti necessari allo svolgimento delle attività in corso.

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'Ente nel corso della propria attività e si colloca, temporalmente, tra l'archivio corrente e l'archivio storico.

I documenti sono trasferiti all'archivio di deposito una volta venuta meno l'esigenza dell'Ente di disporne nel proprio archivio corrente e, comunque, non oltre cinque anni. Si tratta di una fase di sedimentazione della documentazione, ossia di un periodo in cui i documenti esauriscono le proprie funzioni rivelando la propria natura temporanea o permanente, a seconda del valore delle informazioni in essi contenute. Le attività che connotano questa fase d'archivio sono definite dagli artt. 67, 68 e 69 del TUDA e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e di ricerca del materiale (registri di protocollo, piani di classificazione, repertori dei fascicoli, ecc.). I documenti sono conservati rispettando l'organizzazione che essi avevano nell'archivio corrente.

I tempi di conservazione dei documenti nell'archivio di deposito sono individuati tenendo presenti le esigenze di conservazione dei documenti, sia a fini amministrativi sia di ricerca storica. I tempi di conservazione sono fissati sulla base della rilevanza del contenuto dei documenti; per ciò che attiene le esigenze di carattere amministrativo, i tempi di conservazione sono individuati sulla base delle previsioni della normativa, segnatamente in materia di prescrizione legale e di archivi degli enti pubblici, nonché delle specifiche esigenze amministrative del CREA. Nel massimario di scarto sono individuati i criteri e le procedure attraverso i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza archivistica, ai sensi del D.Lgs. 22 gennaio 2004, n. 42, art. 21. Il massimario individua le tipologie documentali in rapporto ai procedimenti nell'ambito dei quali sono realizzate; del massimario è parte integrante il prontuario di scarto, nel quale sono indicati, per ciascuna tipologia documentaria, i tempi di conservazione. Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'ente, avvengono nella fase di deposito, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine. La proposta di scarto formulata su apposito modulo, l'elenco di scarto, in cui sono indicate le tipologie documentarie, gli estremi cronologici e le motivazioni dell'eliminazione è inviata alla Soprintendenza competente per la necessaria autorizzazione.

Sono sottoposte a procedura di scarto le tipologie documentali che hanno maturato il periodo di conservazione fissato nel massimario.

Il Massimario di conservazione e scarto dei documenti del CREA (prima CRA) è stato approvato con Delibera del CdA n. 16 del 24 gennaio 2013 (Allegato 2).

Consultazione

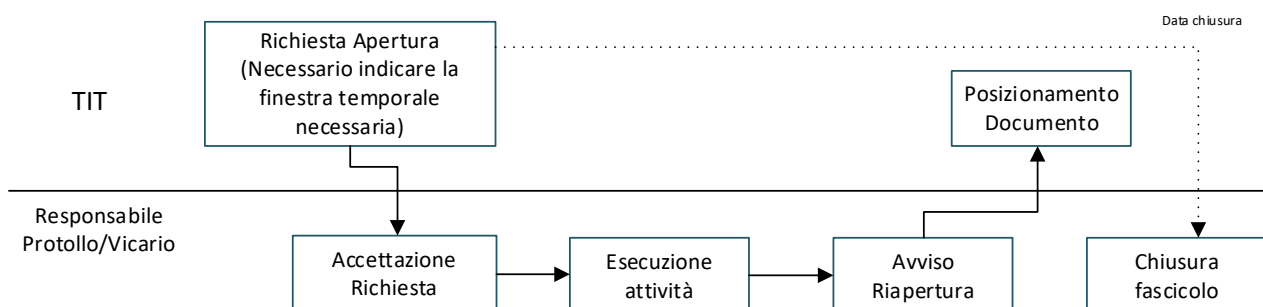
Le modalità di accesso agli archivi sono stabilite da adeguate politiche e procedure improntate a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

Apertura di un fascicolo chiuso

In casi motivati e straordinari, qualora il procedimento o l'attività correlata non possa considerarsi definitivamente conclusa, è possibile procedere alla riapertura di un fascicolo già chiuso.

La riapertura deve essere autorizzata dal Responsabile o da altro soggetto formalmente incaricato. L'operazione comporta l'aggiornamento dello stato del fascicolo da "chiuso" a "aperto" nel sistema di gestione documentale.

In questi casi l'utente TIT (Titolare di Ufficio) invierà una richiesta di apertura del fascicolo al Responsabile della Gestione Documentale o al suo Vicario, in cui è indicata la finestra temporale necessaria per posizionare ulteriori documenti all'interno del fascicolo riaperto (in assenza di indicazione temporale il fascicolo rimarrà aperto 15 giorni). Il Responsabile della Gestione Documentale/Vicario provvederà quindi alla riapertura del fascicolo e successiva chiusura trascorsa la finestra, seguendo i passi riportati in figura.



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

Unicità del protocollo informatico

Il protocollo nelle PA rappresenta “un sistema di certificazione e registrazione della corrispondenza attraverso il quale le amministrazioni pubbliche registrano il transito dei documenti tra l'esterno e l'interno (e viceversa) oppure internamente tra i vari uffici”.

Il registro di protocollo è qualificato atto pubblico originario che fa fede, fino a querela di falso, della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità di esso. La documentazione che non risulta registrata viene considerata giuridicamente inesistente presso l'amministrazione.

Nell'ambito della AOO il registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

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

Il numero di protocollo è costituito da sette cifre numeriche.

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

Non è pertanto consentita, in nessun caso, la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata presso una UOR viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso viene prodotto automaticamente dal SdP e reso disponibile in formato PDF.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il Registro giornaliero di protocollo è inviato in conservazione. Tale operazione viene espletata automaticamente dal SdP.

Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i tipi di documenti informatici trattati dall'AOO (ricevuti, trasmessi ed interni formali).

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

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

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

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento;
- gli eventuali allegati

Prima di procedere alla registrazione di protocollo di un documento informatico sottoscritto con firma digitale, è necessario che sia accertata l'autenticità, la provenienza, l'integrità, la regolarità e la validità amministrativa della firma e, solo in caso di esito positivo della verifica, si potrà procedere alla protocollazione, facendo corrispondere ad ogni documento, comprensivo degli eventuali allegati, una sola registrazione.

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

Tali dati facoltativi sono descritti nei paragrafi seguenti.

Elementi facoltativi delle registrazioni di protocollo

La registrazione di protocollo di un documento, oltre ai dati obbligatori può contenere i seguenti elementi facoltativi:

- le modalità di ricezione / spedizione del documento;
- il collegamento ad altri documenti, metadati specifici relativi ad un acquisto – CIG – e/o ad un progetto - ObFu, Acronimo di progetto. Per le fatture sono automaticamente impostati come metadati tutte le informazioni identificative della fattura.

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo.

La registrazione di valori nei metadati facoltativi del protocollo può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UOR. In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Segnatura di protocollo dei documenti

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

La segnatura di protocollo è l'apposizione, o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo inequivocabile. Per i documenti protocollati in formato PDF è automaticamente prodotta la copia di cortesia con la stampigliatura della segnatura di protocollo. Questa copia, a causa della modifica effettuata per apporre la stampigliatura, sarà un documento con la firma digitale non più valida.

Annullamento delle registrazioni di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata, integrata o cancellata, ma soltanto annullata mediante apposita procedura.

La necessità di modificare, anche un solo campo tra quelli obbligatori della registrazione di protocollo per correggere errori verificatisi in sede di immissione manuale di dati, comporta l'obbligo di annullare l'intera registrazione di protocollo.

L'annullamento non elimina il documento e/o le informazioni relative alla registrazione di protocollo, tutto rimane memorizzato nel SdP. Al momento dell'annullamento, viene predisposto in automatico il *Provvedimento di annullamento* con la motivazione inserita nella richiesta di annullamento. L'operazione è registrata con data e orario nel *Registro degli annullamenti* riportato in calce al *Registro giornaliero di protocollo*. La procedura prevede, inoltre, l'apposizione di un cartellino rosso sul documento in posizione visibile e consente la visualizzazione del documento e la lettura di tutte le informazioni originarie.

Il RSP e l'eventuale vicario appositamente nominato sono autorizzati ad annullare.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica procedura presente nel SdP, adeguatamente motivata, che produce una attività in entrata per il RSP. Quest'ultimo valuta la motivazione e procede all'annullamento.

Analoga procedura di annullamento va eseguita quando, stante le funzioni primarie di certificazione riconosciute dalle norme alla UOP, emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio, originale cartaceo ed e-mail, siano stati attribuiti più numeri di protocollo.

Livello di riservatezza

Ad ogni documento, all'atto della sua registrazione nel sistema di gestione informatica dei documenti, è assegnato un livello di riservatezza, una sorta di Access Control List, che consente di stabilire quali utenti o gruppi di utenti possono avere accesso ad esso.

Il SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.

In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.

Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale. Ciascun utente può accedere solamente ai documenti che ha prodotto o che gli sono stati assegnati direttamente, oppure ai documenti assegnati all'unità organizzativa cui appartiene, o a un ufficio ad esso subordinato.

Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore o uguale. I documenti invece che hanno un livello di riservatezza superiore lo mantengono.

Il livello di riservatezza dei singoli documenti è attribuito all'atto della protocollazione ma può altresì essere successivamente parzialmente modificato e rimane indipendente dal livello di riservatezza del fascicolo.

Casi particolari di registrazione di protocollo

Tutta la corrispondenza diversa da quella di seguito descritta viene regolarmente aperta, protocollata e assegnata con le modalità e le funzionalità proprie del SdP.

Gestione delle registrazioni di protocollo con SdP

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

Il sistema di sicurezza del SdP garantisce la protezione di tali informazioni sulla base della relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

Registrazioni di protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente.

Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

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

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

Descrizione funzionale ed operativa

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo dello stesso.

Rilascio delle credenziali di autenticazione e dei profili di autorizzazione.

L'accesso all'applicativo avviene con le credenziali di autenticazione in uso all'Ente (Autenticazione Microsoft). Gli utenti sono definiti sul SdP ed utilizzano le proprie credenziali di accesso Microsoft. Le utenze sono personali e non assegnate alle funzioni svolte nell'ambito dell'Amministrazione. La persona che subentra nelle funzioni di un'altra (es. il titolare va in pensione e viene sostituito) deve avere utenza propria. Tutte le operazioni sono registrate a nome delle persone che le compiono. Ogni utente abilitato ha un proprio profilo di autorizzazioni, impostato dal Titolare UOR o personale delegato.

Operatore Ufficio di protocollo

Di tutti gli utenti abilitati alla gestione informatica dei documenti, quelli dell'ufficio protocollo sono abilitati allo svolgimento delle seguenti operazioni:

- la registrazione di protocollo dei documenti in arrivo;
- la registrazione di protocollo dei documenti in partenza;
- la registrazione di protocollo dei documenti interni.

12. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Il registro di emergenza

Qualora non fosse possibile fruire del SdP per una interruzione accidentale o programmata, l'Amministrazione è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.

Il registro di emergenza si rinnova ad ogni utilizzo, è identificato dal numero di determinazione che stabilisce l'attivazione del registro e dall'anno.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul registro di protocollo generale.

Il registro di emergenza si configura come un repertorio del protocollo generale.

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini dei procedimenti amministrativi. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento.

Modalità di apertura del Registro di Emergenza

Qualora non fosse possibile fruire del SdP per una interruzione accidentale o programmata, deve essere rilasciata, da parte del RSP, specifica autorizzazione per l'uso del Registro di Emergenza e gli estremi del provvedimento di autorizzazione dovranno essere riportati nel Registro stesso. In ogni caso è data comunicazione al RSP dell'utilizzo del Registro.

Modalità di utilizzo del Registro di Emergenza

Per ogni giornata in cui viene usato il Registro di Emergenza, è riportato sul Registro stesso il numero totale di operazioni registrate. La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico, dal numero successivo all'ultimo registrato prima dell'interruzione.

Modalità di chiusura e di recupero del Registro di Emergenza

Quando viene ripristinata la piena funzionalità del sistema di protocollo informatico, il RSP o suo Vicario provvedono alla chiusura del Registro di Emergenza, annotando il numero delle registrazioni effettuate e la data e l'ora di ripristino della funzionalità del sistema.

Le informazioni relative ai documenti protocollati con il Registro di Emergenza sono inserite nel sistema di protocollo informatico. Nel protocollo informatico saranno riportati tutti i dati trascritti nel Registro di Emergenza: ad ogni protocollo del Registro sarà attribuito un nuovo numero di protocollo, secondo la numerazione del protocollo informatico, ed a questo sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

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

Modalità di approvazione ed aggiornamento del manuale

Il presente Manuale di gestione del protocollo informatico, dei documenti e dell'archivio su proposta del Direttore Generale del CREA è approvato dal Consiglio di Amministrazione.

Il Manuale potrà essere aggiornato a seguito di:

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

Regolamenti abrogati

Con l'entrata in vigore del presente Manuale sono annullati tutti i regolamenti interni all'AOO nelle parti contrastanti con lo stesso.

Pubblicità del presente manuale

Il Manuale è inviato a tutto il personale del CREA ed è pubblicato sul sito istituzionale.

Al fine di assicurarne adeguata conoscenza da parte del personale CREA, verranno organizzati percorsi di formazione in tema di gestione documentale.

Operatività del presente manuale

Il presente Manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

Norme di rinvio

Per quanto non espressamente previsto dal presente Manuale, si farà riferimento alla normativa vigente in materia, adottando comportamenti ispirati ai principi del buon andamento dell'attività amministrativa.