

COMUNE DI BESSUDE

Provincia di SS

MANUALE DI GESTIONE DOCUMENTALE

- 3.7 Corrispondenza di particolare rilevanza e documenti esclusi
- 3.8 Errata ricezione di documenti
- 3.9 Rilascio di ricevute
- 3.10 Classificazione, assegnazione e presa in carico dei documenti
- 3.11 Documentazione particolare
- 3.12 Flusso dei documenti inviati (schema)
- 3.13 Produzione interna dei documenti
- 3.14 Verifica formale dei documenti
- 3.15 Registrazione di protocollo e segnatura
- 3.16 Trasmissione di documenti informatici
- 3.17 Trasmissione di documenti cartacei a mezzo posta
- 3.18 Documenti informali

Parte quarta

La classificazione

- 4.1 Titolare o piano di classificazione
- 4.2 Classificazione dei documenti
- 4.3 La fascicolazione
- 4.4 Assegnazione automatica dei fascicoli digitali ai documenti
- 4.5 Modifica delle assegnazioni dei fascicoli digitali
- 4.6 Chiusura dei fascicoli digitali
- 4.7 Serie archivistiche e repertori

Parte quinta

Registrazione di protocollo

- 5.1 Unicità del protocollo informatico
- 5.2 Registrazione di protocollo
- 5.3 Elementi facoltativi delle registrazioni di protocollo
- 5.4 Segnatura di protocollo dei documenti
- 5.5 Annullamento delle registrazioni di protocollo
- 5.6 Protocollazione documenti interni formali
- 5.7 Oggetti ricorrenti
- 5.8 Registrazione differita di protocollo
- 5.9 Documenti riservati (Protocollo riservato)

Parte sesta

Archiviazione e conservazione

- 6.1 Archiviazione dei documenti - Tempi, criteri e regole di selezione del sistema di classificazione

Allegati

Allegato 1

Aree organizzative omogenee e responsabili della gestione documentale

Allegato 2

Glossario regole tecniche

Allegato 3

Titolario

Allegato 4

Livelli di abilitazione

Allegato 5

Affidatari servizi esternalizzati con gestione documentale e dati

Allegato 6

Elenco dei software utilizzati per la formazione dei documenti informatici

Allegato 7

Modello di carta intestata

Allegato 8

I formati

Allegato 9

Metadati

1.4 Individuazione del/dei responsabile/i della gestione documentale

Con riferimento all'unica AOO si prende atto che con provvedimento n. 15 in data 12/10/2015 è stato individuato nella signora SERRA MARIA TERESA che riveste la qualifica di Istruttore direttivo il Responsabile della gestione documentale, che ha provveduto alla predisposizione del presente manuale, parimenti con il medesimo provvedimento è stato individuato il vicario nella signora CARTA GIOVANNA ANTONIA che riveste la qualifica di Istruttore amministrativo.

1.5 Individuazione del servizio archivistico e per la gestione del protocollo

Nell'ambito dell'unica AOO il Servizio archivistico e per la gestione del protocollo, in conformità alle Regole tecniche e l'archiviazione documentale, è individuato nel servizio protocollo, che svolge le attività previste dal quadro normativo derivante dalle Regole tecniche, dal TU e dal Codice, avvalendosi delle risorse sopra specificate.

1.6 Il titolare di classificazione

La classificazione è un'attività di organizzazione logica di tutti i documenti correnti, protocollati e non (spediti, ricevuti, interni) secondo uno schema di voci che identificano attività e materie specifiche del soggetto produttore.

Il sistema complessivo di organizzazione dei documenti è definito nel titolare di classificazione.

Lo scopo del titolare di classificazione è quello di guidare la sedimentazione dei documenti secondo le funzioni del soggetto. La classificazione collega ciascun documento in maniera univoca a una precisa unità archivistica, il fascicolo.

Il Comune di BESSUDE adotta la classificazione individuata nella Circolare 1° marzo 1897 n. 17100/2 del Ministero dell'Interno (cosiddetta Circolare Astengo).

1.7 Modello operativo adottato per la gestione documentale

La gestione documentale viene posta in essere con un modello operativo che contempla l'attività di vari soggetti:

- gli operatori di settore;
- i responsabili del procedimento che svolgono attività istruttoria;
- i responsabili di procedimento con delega all'emissione di provvedimenti aventi rilevanza esterna;
- i responsabili di servizio/dirigenti;
- soggetti esterni cui è affidata la gestione di servizi.

L'abilitazione e il rilascio delle credenziali (firma elettronica semplice o avanzata basata su username e password o sistemi equivalenti quali OTP etc.) sono gestiti dal servizio archivistico e sono esplicitati nell'apposito allegato.

In relazione all'organizzazione del Comune che prevede l'esternalizzazione di vari servizi si rende necessario consentire agli affidatari dei medesimi la gestione di documenti e dati, anche personali, per conto di questo Comune. Tali soggetti, indicati nell'apposito allegato, vengono individuati quali responsabili del trattamento dei dati personali ai senso

Parte seconda

Il documento e le tipologie documentarie

2.1 Il documento amministrativo – l'originale

L'attività del Comune di BESSUDE viene posta in essere mediante la formazione, la gestione e la conservazione di documenti amministrativi informatici, intesi quale rappresentazione informatica di atti, fatti o stati giuridicamente rilevanti, che costituiscono informazione primaria e originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Solo qualora non sia possibile la formazione di originali informatici per ragioni organizzative o tecniche, anche di natura temporanea, possono essere formati e gestiti documenti analogici, i quali, ai fini della conservazione dovranno essere convertiti, con le modalità indicate nel manuale per la conservazione, in forma digitale.

Per documento analogico si intende un documento amministrativo prodotto su supporto non informatico, di norma su supporto cartaceo.

Il documento analogico è prodotto con strumenti analogici (es. a mano, macchina da scrivere, ecc.) o con strumenti informatici (es. lettera scritta con Word, ecc.). L'originale è analogico, cartaceo e dotato di firma autografa.

In attuazione del combinato disposto degli articoli 23 e 40 del Codice e degli articoli 3 e 9 delle "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" approvate con D.P.C.M 13 novembre 2014 (di seguito indicate come Regole tecniche documento) il Comune di BESSUDE forma gli originali dei propri documenti informatici mediante:

- 1) **Produzione** di documenti mediante l'utilizzo degli **applicativi software** specificatamente indicati nell'apposito allegato, utilizzando i formati individuati dalle Regole tecniche per il protocollo e Regole tecniche documento, o eventuali altri formati illustrati negli appositi allegati in calce;
- 2) **La ricezione** dall'esterno di documenti (istanze, dichiarazioni e comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del Codice) pervenuti mediante:
 - a) **Posta Elettronica Certificata** all'indirizzo indicato sul sito istituzionale di questo Comune, registrato ed aggiornato su www.indicepa.gov.it quando ne sia certa la provenienza ricorrendo almeno una delle seguenti circostanze:
 - Il documento è sottoscritto con **firma digitale** o altro tipo di **firma elettronica qualificata**;
 - Il documento è dotato di segnatura di protocollo informatico;
 - Ovvero sia comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche.
 - b) **Utilizzo di apposite procedure applicative rese disponibili sul sito istituzionale** a condizione che l'autore sia identificato mediante:
 - Sottoscrizione con firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato;

COMUNE DI BESSUDE

Il sottoscritto, nella sua qualità di funzionario delegato dal Sindaco, attesta che la presente copia del documento allegato è stata prodotta mediante l'utilizzo di un sistema di gestione documentale conforme alle regole tecniche vigenti che garantisce la corrispondenza di forma e contenuto all'originale.

Il Funzionario Incaricato
Firmato digitalmente

2.3 Copia analogica di documento informatico

Sistema di gestione documentale NON conforme alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014)

La conformità viene attestata con apposita dichiarazione in calce alla copia, sottoscritta con firma autografa dal funzionario delegato dal Sindaco ad autenticare le copie.

Formula

COMUNE DI BESSUDE

Il sottoscritto, nella sua qualità di funzionario delegato dal Sindaco, attesta che la presente copia del soprariportato documento informatico è conforme all'originale.

Il Funzionario Incaricato
Firma autografa

2.4 Duplicati di documenti informatici

Il duplicato di un documento informatico è un documento informatico risultante dall'utilizzo di un software specifico composto dalla stessa sequenza di bit del documento di origine, cioè un nuovo esemplare dello stesso documento. Il duplicato viene prodotto:

- sullo stesso sistema di memorizzazione: stesso PC o dispositivo mobile
- su altro sistema di memorizzazione: ad esempio da PC a dispositivo mobile (chiavetta USB, CD etc.).

Considerato che è in corso l'adeguamento del sistema di gestione documentale alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014), ai duplicati viene allegata un'attestazione di conformità relativa al processo di formazione del duplicato che assicura l'identità della sequenza di bit del duplicato rispetto all'originale.

COMUNE DI BESSUDE

Il sottoscritto, nella sua qualità di funzionario delegato dal Sindaco, attesta che il duplicato allegato è conforme all'originale.

Il Funzionario Incaricato

- il numero di telefono e l'indirizzo e-mail/PEC dell'unità organizzativa;

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo e data di redazione del documento;
- il numero di protocollo;
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- la firma digitale del Responsabile del Procedimento o del responsabile del provvedimento finale.

Il documento informatico consente l'identificazione dell'amministrazione mittente attraverso l'insieme dei metadati definiti nell'apposito allegato delle regole tecniche di cui alle regole tecniche vigenti.

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica, in primo luogo avvalendosi del sistema di gestione documentale e del portale comunale, moduli e formulari standardizzati validi ad ogni effetto di legge.

I documenti sono gestiti secondo gli standard internazionali.

Per la formazione dei documenti vengono utilizzati i formati esposti nell'allegato alle vigenti regole tecniche.

L'utilizzo di formati diversi deve essere adeguatamente motivato.

2.9 La firma

Nell'ambito del sistema di gestione documentale questo Comune utilizza le seguenti tipologie di firma.

Semplice: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica in forma di PIN o insieme di Username e Password.

La firma semplice viene utilizzata per l'autenticazione a fini di consultazione e accesso all'erogazione di servizi:

- all'interno dell'Ente per l'utilizzo delle procedure documentali dei software applicativi secondo i diversi livelli di autorizzazione (amministratore, operatore, abilitato alla consultazione);
- per la consultazione di fascicoli informatici sul sito dell'Ente in quanto soggetto interessato al procedimento;
- per il download di documentazione dal sito dell'Ente;
- per procedimenti semplici sul sito dell'Ente, ad esempio pagamenti.

Non ha valore di sottoscrizione.

La firma semplice viene rilasciata a tutti gli operatori del sistema di gestione documentale.

Avanzata: consente l'identificazione del firmatario e la connessione univoca ad esso. Le forme di firma avanzata utilizzabili da questo Ente sono: Certificati digitali, codici OTP (One Time Password), firma grafometrica, PEC con ricevuta completa, Carta Id Elettronica, Carta Naz. Servizi.

L'autenticazione avviene anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata.

Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata.

2.11 Immodificabilità e integrità del documento informatico, copie, duplicati ed estratti

L'immodificabilità e l'integrità di documento informatico, copie, duplicati ed estratti viene assicurata mediante:

- a) conversione in formato privo di contenuti dinamici (macro istruzioni e codici eseguibili) quali in PDF/A o altri formati esplicitati nell'apposito allegato;
- b) sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
- c) l'apposizione di una validazione temporale (marca temporale);
- d) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
- e) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
- f) il versamento ad un sistema di conservazione.

Con riferimento in particolare a documenti specifici quali:

- 1) la registrazione di **protocollo**;
- 2) la registrazione in ulteriori **registri, repertori, albi, elenchi, archivi e raccolte di dati** contenuti nel sistema di gestione documentale.

Al documento, una volta divenuto immodificabile, deve essere associato **l'insieme minimo dei metadati** (identificativo univoco e persistente, il riferimento temporale, l'oggetto, il soggetto che ha formato il documento, l'eventuale destinatario, l'impronta informatica). Eventuali ulteriori metadati sono descritti nell'apposito allegato.

2.12 Il fascicolo informatico

Tutti i documenti, originali, copie, duplicati estratti, copie per immagine di documenti cartacei relativi ad ogni singolo procedimento vengono raccolti nel fascicolo informatico che contiene tutti gli atti, i documenti e i dati del procedimento medesimo da chiunque formati.

Il fascicolo informatico viene istituito dal Responsabile del procedimento all'avvio del medesimo, sia nel caso di procedimento ad istanza di parte che d'ufficio, nell'ambito del sistema di gestione documentale.

Dell'istituzione del fascicolo è data immediata comunicazione al servizio protocollo che provvede all'adeguamento del protocollo.

Il fascicolo deve garantire:

- a) la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto e alle finalità, dei singoli documenti che lo compongono;
- b) l'esercizio in via telematica dei diritti di accesso e partecipazione previsti dalla legge 241/1990.

Nel fascicolo informatico i documenti vengono:

possono essere associati ulteriori metadati.

al settore competente oppure - invio del documento mediante mail ordinaria dal protocollo al settore competente	
Valutazione da parte dell'ufficio del documento in ordine alla - forma - ricevibilità - pertinenza	<i>Idem</i>
In caso di erronea attribuzione all'ufficio: restituzione al protocollo per nuova assegnazione	<i>Idem</i>
Acquisizione al fascicolo digitale	<i>Idem</i>
Gestione del documento nel procedimento di competenza.	<i>Idem</i>

3.2 Ricezione di documenti informatici sulle caselle di posta elettronica certificata

La ricezione dei documenti informatici avviene prioritariamente tramite le caselle di posta elettronica certificata.

Ogni messaggio deve riferirsi a una sola questione. Anche nel caso in cui vengano inviati contestualmente più documenti relativi allo stesso oggetto deve essere possibile attribuire all'invio un'unica protocollazione, e un'unica classificazione.

Quando i documenti informatici pervengono all'ufficio protocollo, direttamente dall'esterno o da altri settori qualora il documento sia stato ricevuto sulla casella PEC specifica del settore, il servizio previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo.

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime e accessorie associate ai documenti protocollati.

Le caselle PEC sono controllate quotidianamente, nei giorni di apertura degli uffici, dal servizio protocollo o dai singoli servizi.

I documenti digitali sono resi disponibili agli uffici:

- attraverso il sistema di gestione documentale subito dopo l'operazione di classificazione e smistamento;
- mediante invio per apposita e-mail ordinaria dal protocollo al settore competente.

3.3 Ricezione di documenti informatici sulla casella di posta elettronica ordinaria

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non destinata specificamente al servizio di protocollazione e non PEC o similare, spettano al titolare della casella le valutazioni e le incombenze in merito:

indipendentemente dal supporto utilizzato, è preventivamente inviato in visione al Segretario Generale, che provvede ad individuare l'unità organizzativa o i singoli soggetti competenti a trattare il documento, fornendo eventuali indicazioni riguardo alla gestione del documento stesso.

Sono esclusi dalla registrazione di protocollo:

- bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico e certificazioni anagrafiche;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura.

3.8 Errata ricezione di documenti

- **Digitali:** nel caso in cui pervengano alle caselle e-mail della AOO messaggi istituzionali dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'addetto rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Amministrazione".

- **Cartacei:** nel caso in cui pervengano erroneamente all'Ente documenti indirizzati ad altre amministrazioni o soggetti, possono verificarsi le seguenti eventualità:

- si restituiscono al servizio postale;
- se si tratta di documento cartaceo e la busta viene aperta per errore, il documento è protocollato in entrata e successivamente in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore", provvedendo quindi al rinvio al mittente.

3.9 Rilascio di ricevute attestanti la ricezione di documenti

- **Digitali:** la ricezione di documenti attraverso la casella di posta certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.

Nel caso di invio di documentazione tramite servizi online sul portale dell'Ente viene automaticamente rilasciata dal sistema una ricevuta attestante l'invio della documentazione.

Nel caso di documenti inviati via posta elettronica certificata per la pubblicazione all'Albo pretorio Comunale, la conferma di pubblicazione (se richiesta) potrà essere trasmessa al mittente attraverso lo stesso canale, immediatamente dopo la scadenza della pubblicazione richiesta.

Nessuna ricevuta viene di norma rilasciata o trasmessa in caso di ricezione di documenti tramite posta elettronica ordinaria, salvo specifica richiesta.

- **Cartacei:** il servizio protocollo non rilascia, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. Sono di regola esclusi dalla protocollazione i documenti non indirizzati all'Ente, per i quali lo stesso funge unicamente da tramite tra il mittente e il destinatario finale. Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all'ufficio protocollo ed è richiesto il rilascio di una

documentazione deve consentire di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico.

Ogni registrazione deve riportare necessariamente:

- a) dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- b) dati di classificazione e fascicolazione;
- c) numero di repertorio progressivo e annuale (generato in modo non modificabile).

Nel caso di gare nel mercato elettronico o acquisti effettuati mediante piattaforme informatiche, tutta la documentazione è ricevuta telematicamente direttamente nel sistema, che ne garantisce la sicurezza e riservatezza.

Le offerte di gare d'appalto o altra documentazione da consegnarsi all'Ente in busta chiusa sono registrate al protocollo. Dopo l'apertura della busta a cura dell'ufficio che gestisce la gara verrà riportato su ciascun documento contenuto:

- 1) data apertura busta;
- 2) data e numero di protocollo della busta.

Gli ordinativi informatici sono firmati digitalmente e inviati alla tesoreria la quale provvede, una volta verificata l'autenticità e integrità degli ordinativi, a rilasciare le opportune ricevute di presa in carico e di avvenuto pagamento. Per esigenze organizzative interne, l'ente stampa e conserva una copia dei documenti sottoscritti con firma originale.

Il sistema informatico provvede automaticamente a registrare gli allegati di un documento elettronico.

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi e pertanto da assegnare a più fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente una dall'altra.

L'originale verrà inviato al destinatario indicato nel documento, oppure, nel caso di destinatari plurimi, al primo in indirizzo.

Nel caso in cui l'individuazione di più oggetti venga effettuata successivamente da parte del destinatario, questi deve inviare all'ufficio protocollo apposita comunicazione affinché si provveda nel medesimo modo.

3.14 Verifica formale dei documenti

Le unità organizzative sono autorizzate dal Responsabile della gestione documentale e del Servizio di Protocollo informatico a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita. Le unità organizzative provvedono quindi a eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa.

3.15 Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dalle singole unità organizzative abilitate, in quanto collegate al sistema di protocollo informatico della AOO a cui appartengono.

3.16 Trasmissione di documenti informatici

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

Per la spedizione dei documenti informatici, l'AOO si avvale prioritariamente di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, e di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche. In particolare, la PEC è strumento ordinario di trasmissione verso i cittadini che hanno dichiarato il loro domicilio digitale, nonché verso i soggetti inseriti nell'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti, o in altri indici analoghi che si rendessero disponibili in futuro.

In caso di più destinatari riferiti a un unico numero di protocollo, si generano tante PEC quanti sono i destinatari.

È ammesso il recapito tramite posta elettronica tradizionale, qualora si disponga dei necessari riferimenti relativi al destinatario.

Nel caso di trasmissione di allegati al documento che eccedano la capienza della casella di posta elettronica, è possibile utilizzare supporti rimovibili, o avvalersi di adeguati canali telematici alternativi.

La trasmissione telematica mediante posta elettronica certificata ha effetto equivalente alla notificazione per mezzo della posta raccomandata.

3.17 Trasmissione di documenti cartacei a mezzo posta

L'ufficio protocollo gestisce le operazioni di spedizione della corrispondenza predisposta dagli uffici comunali. Gli uffici comunali recapitano al protocollo i plichi da spedire, in tempo utile per consentire di organizzare al meglio la gestione.

L'ufficio protocollo effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza cartacea e cura il costante monitoraggio della spesa e verifica la disponibilità delle necessarie risorse economiche, informando con congruo anticipo il Responsabile del servizio dell'imminente esaurimento dei fondi a disposizione.

Il Responsabile della gestione documentale e del Servizio di Protocollo informatico

Parte quarta

La classificazione

4.1 Titolario o piano di classificazione

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti gestiti".

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza di leggi o regolamenti.

Le modifiche al Titolario sono apportate con provvedimento esplicito della funzione di governo dell'amministrazione.

La revisione anche parziale del Titolario viene proposta dal RSP quando necessaria e opportuna.

Dopo ogni modifica del Titolario, il Responsabile del protocollo provvede a informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Viene garantita la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

Per ogni modifica di una voce, viene riportata la data di introduzione e la data di variazione. Le variazioni sono di norma introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolario, e valgono almeno per l'intero anno.

4.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è generalmente strutturata a livelli che si articolano gerarchicamente tra loro.

Le voci di primo e secondo livello del titolario (titoli e classi) individuano le funzioni primarie e di organizzazione dell'Ente.

I titoli e le classi sono già forniti nel sistema informatico di protocollo e gestione documentale.

I successivi livelli di classificazione (macro-fascicoli, fascicoli, sotto-fascicoli...) corrispondono a specifiche competenze che rientrano concettualmente nelle macrofunzioni descritte dai primi livelli.

Le operazioni di classificazione vengono generalmente svolte in momenti diversi e da

4.4 Serie archivistiche e repertori

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.

Il repertorio è costantemente aggiornato.

- l'oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- la classificazione;
- l'impronta del documento informatico.

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

5.3 Elementi facoltativi delle registrazioni di protocollo

Il Responsabile Servizio Protocollo, con proprio provvedimento e al fine di migliorare la gestione, la ricerca e la conservazione della documentazione, può modificare e integrare gli elementi facoltativi del protocollo, anche per singole categorie o tipologie di documenti.

La registrazione degli elementi facoltativi del protocollo, previa autorizzazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico, può essere modificata, integrata e cancellata in base alle effettive esigenze delle unità organizzative o del servizio protocollo. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

5.4 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.

Le informazioni previste sono:

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'area organizzativa omogenea (AOO) individuata ai fini della registrazione e della gestione documentale;
- il codice identificativo dell'amministrazione;
- il codice identificativo dell'area organizzativa omogenea;
- il codice identificativo del registro di protocollo;
- l'anno solare di riferimento del protocollo;
- titolo e classe di riferimento;
- il numero progressivo di protocollo, costituito da almeno sette cifre numeriche;
- la data di protocollo;
- sigla dell'unità/settore a cui il documento è assegnato per competenza e responsabilità;
- sigle delle unità/settori in copia conoscenza.

Per i documenti analogici le informazioni di cui sopra vengono riportate sul documento attraverso il timbro di registrazione di protocollo.

5.9 Documenti riservati (Protocollo riservato)

Sono previste particolari forme di riservatezza per i documenti relativi a procedimenti disciplinari nei confronti dei dipendenti, vicende o a fatti privati, politici o giudiziari (giudizi pendenti) o documenti che richiedono, comunque, una trattazione riservata. Per tali atti sul registro di protocollo generale compare solo il numero attribuito a ciascun documento e l'annotazione "Riservato".

I documenti registrati con tali forme appartengono al cosiddetto "protocollo riservato" costituito dalle registrazioni il cui accesso è autorizzato solo alle persone espressamente abilitate. Queste ultime hanno comunque la visibilità dei soli documenti riservati trattati dall'unità di appartenenza. Le procedure adottate per la gestione dei documenti ad accesso riservato, comprese le registrazioni, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti.

- b) Statuti, Regolamenti, Decreti, Ordinanze, Interpellanze, interrogazioni, mozioni, Verbali Nucleo di Valutazione, Provvedimenti dirigenziali, Registro di protocollo, Registro albo pretorio, Registro notifiche, Atti relativi a partecipazione societarie – Documentazione relativa alle elezioni amministrative, Atti e documenti del contenzioso legale, schedari, rubriche e repertori dell'archivio, Atti relativi a riordinamenti e scarti archivistici;
 - c) provvedimenti costitutivi, modificativi o estintivi di posizioni giuridiche e quindi anche determinazioni, concessioni, autorizzazioni, nulla osta etc.;
 - d) documenti relativi all'attività contrattuale: Contratti - Verbali di gara - Bandi di gara - Offerta dell'impresa aggiudicataria - Capitolati di gara - Documentazione relativa alla qualificazione;
 - e) documenti prodotti da terzi ma con efficacia costitutiva di diritti soggettivi o abilitativi all'esercizio di attività quali ad esempio segnalazioni certificate di inizio attività (SCIA) etc.;
 - f) i "registri", ovvero quei documenti "sui quali vengono annotati in sequenza, secondo criteri predefiniti (tendenzialmente cronologici), una pluralità di fatti o atti giuridici" (es. il registro delle notifiche, il registro del protocollo, il registro degli infortuni, il repertorio dei contratti);
 - g) tutti i documenti sottoscritti con firma digitale;
 - h) tutti i documenti inviati e ricevuti con posta elettronica certificata;
 - i) studi e relazioni tecniche, ricerche, pubblicazioni, documentazione fotografica, che siano propedeutici a piani, programmi e delibere di carattere generale.
- 2) Documenti da conservare 40 anni:
- a) Mandati di pagamento e reversali di riscossione.
- 3) Documenti da conservare per 15 anni:
- a) Strumenti urbanistici e documenti correlati.
- 4) Documenti da conservare per 10 anni:
- a) i processi verbali relativi a sanzioni elevate nella materia di competenza dell'Ente (polizia amministrativa, commerciale, codice della strada, abusi edilizi); offerte delle ditte non aggiudicatarie, libri contabili etc.;
 - b) Concorsi (domande di partecipazione, elaborati scritti/pratici conservando eventualmente campionatura) – Gestione fiscale e assicurativa dei dipendenti e collaboratori (CUD, modello 730/4, denunce contributive annuali, autoliquidazione Inail, modelli di versamento ai fini contributivi previdenziali e fiscali, cedolini buste paga mensili, denuncia Statistiche sul personale.
- 5) Documenti soggetti a conservazione per 5 anni sono:
- a) le richieste e la documentazione allegata, le pezze giustificative, i rendiconti relativi ai "contributi" ovvero le elargizioni di denaro – comunque denominate – erogate dall'Ente;
 - b) la corrispondenza di carattere occasionale (le cosiddette "carte varie") ovvero "il complesso delle lettere e delle note scritte, inviate e ricevute dall'Ente" con riferimento ad un affare individuato ma che, per la loro scarsa importanza non siano sfociate in una delibera o provvedimento di altro genere, rimaste per così dire senza seguito;

Il processo di conservazione si articola nelle seguenti fasi:

- 1) acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- 2) verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nelle regole tecniche;
- 3) trasmissione del pacchetto di versamento in modalità sicura;
- 4) preparazione, sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del D.P.C.M. e secondo le modalità riportate nel manuale della conservazione;
- 5) preparazione e sottoscrizione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;
- 6) ai fini della interoperabilità tra sistemi di conservazione, produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;
- 7) produzione di duplicati informatici o di copie informatiche effettuata su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
- 8) produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11 del D.P.C.M., in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
- 9) scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore.

6.4 Il sistema di conservazione organizzato e operativo nell'Ente

La conservazione dei documenti prodotti e detenuti da questo Comune verrà effettuata:

mediante organizzazione del servizio di conservazione. La definizione delle modalità di svolgimento della conservazione viene pertanto demandata ad apposito documento che verrà successivamente approvato.

6.5 Specificità per la conservazione del registro di protocollo informatico

In adempimento a quanto previsto dalle regole tecniche l'Ente provvede ad effettuare la conservazione del registro giornaliero di protocollo utilizzando il sistema di conservazione generale dell'Ente.

L'operazione di conservazione del registro di protocollo comprende:

- la predisposizione dell'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno;
- la trasmissione entro la giornata lavorativa successiva, al sistema di conservazione, garantendo l'immodificabilità del contenuto.

Il responsabile di protocollo, direttamente o tramite suoi incaricati, provvede tramite specifica procedura del sistema di protocollo, alla creazione del pacchetto di versamento del registro di protocollo del giorno precedente, per la verifica e la trasmissione al sistema

Parte settima

Registro di emergenza

7.1 Utilizzo del registro di emergenza

Il responsabile del servizio di protocollo informatico autorizza lo svolgimento delle operazioni di registrazione di protocollo sull'apposito registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.

Il registro di emergenza è unico ed è gestito dall'Ufficio Protocollo. Tutti i servizi comunali, in caso di necessità, fanno quindi riferimento a questo ufficio per ottenere l'assegnazione di un numero di protocollo di emergenza, in entrata o in uscita.

Il registro di emergenza si rinnova ogni anno solare, pertanto inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Si applicano le seguenti modalità di registrazione e di recupero dei dati:

- sul registro di emergenza sono riportate le cause, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- per ogni giornata di registrazione in emergenza è riportato sul registro il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollati in emergenza sono inserite immediatamente nel sistema di protocollo informatico ripristinato;
- durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, annotando nella scheda di protocollo gli elementi necessari a mantenere stabilmente la correlazione univoca con il numero attribuito in emergenza.

- piano di continuità del servizio con particolare riferimento sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei “moduli” (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. *separazione della parte anagrafica da quella “sensibile”*) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l’ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l’arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto, dalle forze dell’ordine.

8.2 Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l’impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l’identificazione dell’utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password) (firma elettronica semplice);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow effettuabili alle sole funzioni necessarie (consultazione dei documenti, gestione dei documenti e procedure, amministratore di sistema). A tale proposito si differenziano:
 - utenti interni alla AOO: i livelli di autorizzazione per l’accesso alle funzioni del sistema di protocollo informatico e gestione documentale sono attribuiti dal Responsabile del protocollo dell’amministrazione/AOO. Tali livelli si distinguono

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici.

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

8.4 Trasmissione e interscambio dei documenti informatici

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

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 e i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'amministrazione (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/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 di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

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.

8.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

Parte nona

Norme transitorie e finali

9.1 Modalità di approvazione e aggiornamento del manuale

Il Manuale sarà 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 rilevata nello svolgimento delle attività correnti;
- introduzione di nuove procedure.

Il Manuale viene approvato e modificato con deliberazione della Giunta.

Gli allegati sono modificati, di norma e fatte salve le eccezioni esplicitamente dichiarate, con provvedimenti del Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

9.2 Pubblicità del manuale

Il Manuale, a norma dell'art. 15 della legge n. 15 del 2005, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

Inoltre copia del presente Manuale è:

- resa disponibile a tutto il personale dell'AOO tramite il sistema di gestione documentale;
- inviata all'organo di revisione;
- pubblicata sul sito internet dell'Amministrazione.

9.3 Entrata in vigore

Il presente documento diviene efficace al conseguimento dell'eseguibilità della deliberazione di approvazione.

Allegato 2

Glossario regole tecniche

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizioni del citato decreto e a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

Accesso: operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.

Accreditamento: riconoscimento, da parte dell'**Agenzia per l'Italia digitale**, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione.

Affidabilità: caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.

Aggregazione documentale informatica: aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

Archivio: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività.

Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.

Area organizzativa omogenea: un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.

Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico: dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.

Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.

Base di dati: collezione di dati registrati e correlati tra loro.

Certificatore accreditato: soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, **dall'Agenzia per l'Italia digitale**, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Ciclo di gestione: arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.

informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Generazione automatica di documento informatico: formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.

Identificativo univoco: sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.

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

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*.

Insieme minimo di metadati del documento informatico: complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo e inalterato.

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.

Log di sistema: registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.

Manuale di conservazione: strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione.

Manuale di gestione: strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni.

Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.

Metadati: insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto.

Pacchetto di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione.

Pacchetto di distribuzione: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta.

Pacchetto di versamento: pacchetto informativo inviato dal produttore al sistema di

professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Responsabile della conservazione: soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione.

Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Responsabile della sicurezza: soggetto al quale compete la definizione delle soluzioni tecniche e organizzative in attuazione delle disposizioni in materia di sicurezza.

Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse **storico** culturale.

Sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.

Sistema di conservazione: sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice.

Sistema di gestione informatica dei documenti: nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.

Staticità: Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.

Transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.

Testo unico: decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.

Ufficio utente: riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.

Utente: persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

Versamento agli archivi di stato: operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Allegato 4 Livelli di abilitazione

Nome Utente	Cognome Utente	Area/Ufficio	Servizio	Mansioni	Procedura (applicativo)	Livelli di Abilitazione per l'accesso alle procedure	Modalità di accesso alle procedure
MARIA TERESA	SERRA	AMM.VA-CULTURALE-AA.GG.	DEMOGRAFICI-SEGRETERIA-	RESPONSABIL E	DATAGRAPH	Gestione	altro
GIOVANNA ANTONIA	CARTA	AMMINISTRATI VA-CULTURALE-AA.GG.	PROTOCOLLO	ISTRUTTORE AMMINISTRATIVO	DATAGTAPH	Gestione	altro
SERAFINO	CHESSA	SERVIZI FINANZIARI	GESTIONE ECONOMICO-FINANZIARIA-TRIBUTI-ECONOMATO	RESPONSABIL E	DATAGRAPH	Gestione	altro
PIETRO	SOTGIU	SERVIZI TECNICI	URBANISTICA-LAVORI PUBBLICI-EDILIZIA PUBBLICA E PRIVATA-SUAP	RESPONSABIL E	DATAGRAPH	Gestione	altro
GINA	CAMBONI	SOCIALE	SERVIZI SOCIO-ASSISTENZIALI	ISTRUTTORE AMM.VO	DATAGRAPH	Gestione	altro
ANNA MARIA GIULIA	PIREDDU	SEGRETERIA	SEGRETERIA	SEGRETARIO	DATAGRAPH	Gestione	altro

Allegato 6

Elenco dei software utilizzati per la formazione dei documenti informatici

Scheda A)

Software realizzato all'interno del Comune o open source

Denominazione del software	Servizi / settori di utilizzo	Procedimenti	Tipologia di documenti prodotti
----------------------------	-------------------------------	--------------	---------------------------------

In caso di produzione del software interna all'ente indicare inoltre:

- 1) descrizione dei **formati** utilizzati con specificazione della conformità o meno ai formati di cui all'allegato 2 delle Regole tecniche sulla formazione dei documenti o indicazione dei diversi formati utilizzati con esplicitazione delle motivazioni a base di tale scelta;
- 2) descrizione degli **standard e specifiche tecniche** dei software utilizzati e con specificazione della conformità o meno ai formati di cui all'allegato alle Regole tecniche documento e Regole tecniche protocollo;
- 3) descrizione dei **metadati associati** ai documenti e fascicoli con specificazione della conformità o meno ai formati di cui all'allegato 5 alle regole tecniche in argomento.

Scheda B)

Software e sistemi di gestione documentali acquisiti in licenza d'uso:

Denominazione del software	Servizi / settori di utilizzo	Procedimenti	Tipologia di documenti prodotti	Acquisizione della dichiarazione di conformità
DATAGRAPH	TUTTE LE AREE	PROTOCOLLO		Si
DATAGRAPH	TUTTE LE AREE	DELIBERE- DETERMINE		Si
DATAGRAPH	RAGONERIA- TRIBUTI	CONTABILITA'- BILANCIO- TRIBUTI		Si

Allegato 8

I formati

Il presente documento fornisce indicazioni iniziali sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.

I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali. Il presente documento, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e pubblicato online sul sito dell'Agenzia per l'Italia digitale.

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].docx identifica un formato testo di proprietà della Microsoft;
2. I metadati espliciti: l'indicazione "application/msword" inserita nei tipi MIME che indica un file testo realizzato con l'applicazione Word della Microsoft
3. il *magic number*: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione. Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

In particolare, volendo fare una prima sommaria, e non esaustiva, catalogazione dei più diffusi formati, secondo il loro specifico utilizzo possiamo elencare:

- Testi/documenti (DOC, HTML, PDF,...)
- Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)
- Suoni (MP3, WAV, ...)
- Video (MPG, MPEG, AVI, WMV,...)
- Eseguibili (EXE, ...)
- Archiviazione e Compressione (ZIP, RAR, ...)

fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la gestione del maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

È facilmente comprensibile come, nella fase di gestione del digitale, l'utente debba avere a disposizione la massima flessibilità possibile in termini di formati e funzionalità disponibili. Gli unici limiti sono quelli che un'organizzazione impone a se stessa quando, per esigenze di interscambio e interoperabilità, può determinare i formati e i relativi programmi di gestione che maggiormente soddisfano le contingenti esigenze operative.

Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono.

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura
2. sicurezza
3. portabilità
4. funzionalità
5. supporto allo sviluppo
6. diffusione

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.

Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso, tuttavia, si confida che questi ultimi garantiscano l'adeguatezza e la completezza delle specifiche stesse.

Nelle indicazioni di questo documento si è inteso privilegiare i formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e ETSI.

La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

Allegato 9

Metadati

1. Introduzione

Il presente allegato illustra la struttura dei metadati relativi al documento informatico, al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

2. Metadati minimi del documento informatico

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="documento">
<xs:complexType>
<xs:sequence>
<xs:element name="datachiusura" type="xs:date"/>
<xs:element name="oggettodocumento" type="xs:string"/>
<xs:element name="soggettoprodotto">
<xs:complexType>
<xs:sequence>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="codicefiscale" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="destinatario">
<xs:complexType>
<xs:sequence>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="codicefiscale" type="xs:string"/> </xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="IDDocumento" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

Informazione	Valori Ammessi	Tipo dato	xsd
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri	<xs:attribute name="IDDocumento" type="xs:string" use="required"/>
Definizione			
<i>Identificativo univoco e persistente: è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di</i>			

Informazione	Valori Ammessi	Tipo dato	xsd
Destinatario	nome: Testo libero	Alfanumerico 40 caratteri	<pre><xs:element name="destinatario"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element></pre>
	cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: CodiceFiscale (Obbligatorio, se disponibile)	Alfanumerico 16 caratteri	
Definizione			
<i>Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico.</i>			

3. Metadati minimi del documento amministrativo informatico

L'insieme minimo dei metadati del documento amministrativo informatico è quello indicato agli articoli 9 e 19 delle regole tecniche per il protocollo informatico di cui al D.P.C.M. 31 ottobre 2000 e descritti nella Circolare AIPA del 7 maggio 2001, n. 28.

4. Metadati minimi del fascicolo informatico o della aggregazione documentale informatica

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="fascicolo">
<xs:complexType>
<xs:sequence>
<xs:element name="IPAtitolare" type="xs:string" maxOccurs="1"/>
<xs:element name="IPApartecipante" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/> <xs:element name="responsabile">
<xs:complexType>
<xs:sequence>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="codicefiscale" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="oggettofascicolo" type="xs:string"/>
<xs:element name="documento" type="xs:string" maxOccurs="unbounded"/>
</xs:sequence>
<xs:attribute name="IDFascicolo" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```


Informazione	Valori Ammessi	Tipo dato	xsd
Responsabile del procedimento	nome: Testo libero	Alfanumerico 40 caratteri	<pre><xs:element name="responsabile"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element></pre>
	cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: CodiceFiscale	Alfanumerico 16 caratteri	
Definizione			
<i>Responsabile del procedimento</i>			

Informazione	Valori Ammessi	Tipo dato	xsd
Oggetto	Testo libero	Alfanumerico 100 caratteri	<pre><xs:element name="oggettodefascicolo" type="xs:string"/></pre>
Definizione			
<i>Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Duplic Core prevede l'analoga proprietà "Description" che può includere, ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.</i>			

Informazione	Valori Ammessi	Tipo dato	xsd
Documento	<i>Identificativo del documento così come definito di al capitolo 3.</i>	Alfanumerico 20 caratteri	<pre><xs:element name="documento" type="xs:string" maxOccurs="unbounded"/></pre>
Definizione			
<i>Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità.</i>			