Comune di Arpaise
Provincia di Benevento

Manuale
di
gestione documentale
(art. 5 DPCM 3/12/2013)

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Il presente manuale di gestione documentale, redatto ai sensi dell'art. 5 del DPCM 03/12/2013, descrive il sistema di gestione dei documenti informatici che l'Amministrazione adotta, anche ai fini della conservazione, e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi all'interno dell'Ente.

Proposto

Responsabile per la gestione documentale: dott.ssa Orsola Marra

Adottato

Con Disposizione del Sindaco n. 45 del 23/10/2015

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20/10/2015	Maria Pia Papa	Predisposizione schema

INDICE

1. PRESENTAZIONE DEL MANUALE

1.1 Scopo e ambito di applicazione

Il presente Manuale è adottato ai sensi dell'art. 3, comma d) e dell'art. 5 del Decreto del Presidente del Consiglio dei Ministri 3/12/2013 avente ad oggetto "Regole tecniche per la registrazione e segnatura di protocollo".

In attuazione dell'art. 5, comma 1 del citato DPCM, esso descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Più specificamente effettua una regolamentazione delle attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che della gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Comune.

Il manuale si pone lo scopo di rendere più efficiente la gestione del flusso informativo e documentale interno all'Amministrazione, anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

Esso è adottato su proposta del *Responsabile per la Gestione documentale*.

1.2 Struttura e gestione del manuale

Il Manuale rappresenta il documento di più alto livello del Sistema per la gestione informatica dei documenti, ha lo scopo di documentare le modalità con cui l'Ente ha recepito i requisiti della normativa di riferimento in termini di applicabilità alla propria realtà e costituisce il vademecum per tutti gli operatori comunali che quotidianamente lavorano con i documenti di ufficio.

L'impostazione del documento si ispira sia alla norma UNI EN ISO 9001-2008 "Sistemi di gestione per la Qualità" sia alle linee guida impartite dall'Agenzia per l'Italia Digitale (AgID) (rif. pubblicazione CNIPA del 2006 sulla rivista "i Quaderni", nr. 21).

Il Manuale mira innanzitutto a rispondere a tutti i requisiti normativi impegnando l'Ente al relativo soddisfacimento per le parti applicabili ed, inoltre, fornisce gli opportuni riferimenti alle informazioni di dettaglio, ove sono descritte le procedure organizzative, le modalità operative stabilite dall'Ente, le attività svolte, le responsabilità affidate ed i risultati delle attività (documenti da produrre come output delle attività).

Esso è strutturato in capitoli che, in taluni casi, fanno riferimento ad allegati. Questi ultimi contengono dettagli gestionali e operativi ed appartengono a specifiche tipologie di documentazione che possiamo individuare nelle seguenti:

1. ***Piani***
2. ***Procedure organizzative***
3. ***Istruzioni operative***
4. ***Schemi***
5. ***Moduli***

Gli allegati al Manuale di gestione hanno anche lo scopo di evitare l'iter di approvazione formale del Manuale stesso a seguito di variazioni minime.

Piani
Sono documenti di programmazione che specificano un insieme di scelte e regole, solitamente organizzate nel tempo, per il conseguimento di un determinato obiettivo nel futuro.

Procedure organizzative
Sono i documenti che definiscono concettualmente le attività da eseguire, chiarendo anche le relative responsabilità coinvolte e la documentazione da produrre (risultati/output delle attività). Le procedure organizzative sono espresse ad un livello di dettaglio sufficiente, valutato in relazione all'esperienza del personale interno all'Ente, e in alcuni casi possono far riferimento ad istruzioni operative.

Istruzioni Operative
Le *istruzioni operative* forniscono, là dove necessario, informazioni di maggior dettaglio rispetto alle procedure organizzative; esse contengono informazioni di tipo tecnico-operativo quali mansionari, informazioni o parametri da raccogliere, elenchi di elementi da verificare, sequenze di operazioni elementari, ecc.

Schemi
Si tratta di modelli di documenti importanti da produrre nel corso delle attività (si pensi ad esempio ad uno schema di "contratto" o ad uno schema di "definizione di incarico"). Tali documenti sono di norma piuttosto articolati e pertanto la loro stesura risulta facilitata dalla disponibilità di schemi predefiniti che contengano tutti gli elementi da considerare in fase di redazione e siano facilmente personalizzabili a seconda delle esigenze e dei criteri definiti negli schemi stessi.

Moduli
La modulistica rappresenta l'elemento più atomico del Manuale di Gestione ed è utilizzato nel corso delle varie attività/procedimenti con lo scopo sia di conservare informazioni sia di attestare l'esecuzione di determinate attività. La struttura dei moduli è tale per cui la loro compilazione garantisce la raccolta di tutte le informazioni necessarie in relazione ai vari contesti in cui sono utilizzati. I moduli sono particolarmente importanti in quanto spesso rappresentano le interfacce per la comunicazione tra l'Ente e la cittadinanza. Nel presente Manuale vengono prodotti *schemi* e *moduli* che si ritengono utili a facilitare procedimenti specificati all'interno delle Procedure Organizzative e delle Istruzioni Operative predisposte.

Il presente Manuale non è un documento statico, ma in evoluzione continua, in quanto rappresenta lo strumento per un miglioramento costante nel tempo che, attraverso raffinamenti successivi da apportare all'organizzazione, permetta all'Ente di raggiungere una sempre più efficiente ed efficace gestione informatica dei flussi documentali.

Nella seconda pagina del Manuale e di tutti i suoi allegati, prima dell'indice, è riportata una tabella che evidenzia lo stato delle revisioni fatte dal gruppo di lavoro ed una sintetica descrizione delle modifiche apportate di volta in volta.

Lo stato di revisione del documento è contraddistinto da due numeri progressivi (Rev. xx.xx): il primo numero viene incrementato in caso di modifiche sostanziali al documento,

mentre il secondo è incrementato in caso di modifiche di minore rilevanza. A fianco al numero di revisione viene sempre indicata la data di emissione della revisione del documento, l'autore della modifica e la motivazione dell'aggiornamento.

Il Responsabile per la "*Gestione documentale*" propone alla Giunta Comunale lo schema di manuale da adottare e, successivamente, ne cura la tenuta e l'aggiornamento nel tempo, quindi si fa carico della corretta applicazione e conservazione dello stesso, nonché della sua distribuzione e pubblicazione.

2. DISPOSIZIONI GENERALI

2.1 Riferimenti normativi

La legge sulla trasparenza amministrativa (Legge 241/90), insieme alla validità giuridica del documento elettronico sancita dalla Legge 59/1997, ha dato l'avvio ad una radicale rivoluzione digitale nella Pubblica Amministrazione. Tale rivoluzione trova il suo fondamento legislativo in una serie di norme che regolano la dematerializzazione, il protocollo informatico, la gestione dei flussi documentali, la conservazione dei documenti informativi, e l'accessibilità.

Nel seguito si richiamano le principali norme che costituiscono il quadro legislativo cui dovrà uniformarsi l'Ente.

Il riferimento principale è sicuramente il Codice dell'Amministrazione Digitale (in seguito denominato anche CAD o Codice), emanato con Decreto legislativo del 7 marzo 2005, n. 82, e pubblicato sulla Gazzetta ufficiale n. 112 del 16 maggio 2005. Il Codice ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modo digitale utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione e nei rapporti tra amministrazioni, cittadini ed imprese.

La seduta del Consiglio dei Ministri del 19 Febbraio 2010 ha approvato un Decreto Legge che definisce il nuovo Codice dell'Amministrazione Digitale, in attuazione dei criteri di delega contenuti nell'articolo 33 della legge n. 69 del 2009.

Dematerializzazione

Il termine "dematerializzazione" identifica il processo di sostituzione della documentazione amministrativa, solitamente cartacea, in favore del documento informatico. Nell'ultimo decennio il termine è entrato nel lessico della gestione documentale e nella normativa, che gli ha conferito pieno valore giuridico.

Di seguito si richiamano le principali norme in materia:

1. D.P.C.M. del 13 novembre 2014, "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli artt. 20, 22, 23-bis, 23-ter, 40, comma1, 41 e 71, comma 1, del CAD".
2. Circolare n. 62 del 30 aprile 2013: "Linee guida per il contrassegno generato elettronicamente ai sensi dell'art. 23-ter, comma 5 del CAD.
3. D.P.C.M. 22 febbraio 2013: Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
4. D.P.C.M. del 3 dicembre 2013, recante regole tecniche per la conservazione.

5. DECRETO LEGISLATIVO 30 dicembre 2010 , n. 235, recante modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
6. Deliberazione CNIPA 19 febbraio 2004, n. 11, recante le regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
7. Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 - “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.”.
8. Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42).
9. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR 28 dicembre 2000, n. 445).

Protocollo Informatico

Il Legislatore (DPR 445/2000, art.1) definisce il protocollo informatico come “l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti”, ovvero tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali.

Segue la normativa di riferimento:

1. D.P.C.M. del 13 novembre 2014, “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli artt. 20, 22, 23-bis, 23-ter, 40, comma1, 41 e 71, comma 1, del CAD”.
2. D.P.C.M. del 3 dicembre 2013, recante regole tecniche per la registrazione e segnatura di protocollo.
3. Direttiva del Ministro per l’innovazione e le tecnologie 4 gennaio 2005, punto 2 - “Linee guida in materia di digitalizzazione dell’amministrazione.”
4. Direttiva del Ministro per l’innovazione e le tecnologie 18 dicembre 2003, punto 3, lett. c) - “Linee guida in materia di digitalizzazione dell’amministrazione per l’anno 2004.”
5. Circolare AIPA 21 giugno 2001, n. 31 - "Art. 7, comma 6, del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, recante 'Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428'- Requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente."
6. Circolare AIPA 7 maggio 2001, n. 28 - “Art. 18, comma 2, del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272, recante regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati.”
7. Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.”

8. Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - “Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.”
9. Legge 15 marzo 1997, n. 59, art. 15, comma 2 - “Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa.”

Flussi documentali

I sistemi di gestione dei flussi documentali coordinano tutte le operazioni che riguardano l’elaborazione e la trasmissione dei documenti, specificando le attività ed i ruoli di tutti gli appartenenti al processo di lavoro. Un tale sistema segue un documento durante tutto il suo ciclo di vita, fornendo un’azione di controllo costante per il suo trattamento.

I principali riferimenti normativi sono:

1. D. L. n. 90/2014, art. 24, comma 3-bis, recante “Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari” che favorisce l’interazione tra la pubblica amministrazione e l’utenza attraverso la completa informatizzazione delle operazioni inerenti alla presentazione per via telematica di istanze, dichiarazioni, segnalazioni e altri documenti analoghi da parte della cittadinanza;
2. Direttiva del Ministro per l’innovazione e le tecnologie 9 dicembre 2002 - “Trasparenza dell’azione amministrativa e gestione elettronica dei flussi documentali.”
3. Direttiva del Ministro per l’innovazione e le tecnologie 21 dicembre 2001 - “Linee guida in materia di digitalizzazione dell’amministrazione.”
4. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A).”
5. Direttiva del Presidente del Consiglio dei Ministri 28 ottobre 1999 - “Gestione informatica dei flussi documentali nelle pubbliche amministrazioni.”

Conservazione Documenti Informatici

Come richiamato in precedenza, la Legge 59/1997 riconosce per la prima volta piena validità giuridica al documento informatico; successive modifiche ed integrazioni hanno poi puntualizzato il concetto, stabilendo che il documento informatico ha efficacia probatoria, ma la provenienza delle dichiarazioni ivi contenute è provata solo se sottoscritto con firma digitale ed è prodotto secondo specifiche prescrizioni tecniche. Le caratteristiche principali di un documento informatico valido, sono l'immodificabilità e la leggibilità nel tempo, indipendentemente dal software utilizzato per produrlo.

Seguono i principali riferimenti normativi:

1. D.P.C.M. 13 novembre 2014 “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell’Amministrazione Digitale di cui al decreto legislativo n. 82 del 2005.
2. Circolare n. 65 del 10 aprile 2014, recante le “Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all’art. 44-bis, comma 1, del D.Lgs. 7 marzo 2005, n. 82.

3. D.P.C.M. 3/12/2013 “Regole tecniche per la conservazione”.
4. CIRCOLARE 29 dicembre 2011, n. 59, “Modalita' per presentare la domanda di accreditamento da parte dei soggetti pubblici e privati che svolgono attivita' di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.” (GU n. 32 del 8-2-2012)
5. Decreto legislativo 22 gennaio 2004 - “Codice dei beni culturali e del paesaggio, ai sensi dell’articolo 10 della legge 6 luglio 2002, n. 137.”
6. Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 - “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.”

2.2 Documenti di riferimento

Nella tabella seguente sono indicati anche gli adempimenti precedenti effettuati dall’Ente.

	Descrizione
Disposizione del Sindaco n. 44 del 23/10/2015	Nomina Responsabile del Servizio di Gestione Documentale ai sensi dell’art. 3 comma b) del DPCM del 3/12/2013.

2.3 Allegati da personalizzare in base alle esigenze organizzative dell’Ente

Tipo	Descrizione
Piano	Piano di Sicurezza
Piano	Piano di formazione per il personale dell’Amministrazione
Piano	Piano di conservazione dell’archivio
Procedura Organizzativa	Aree Organizzative Omogenee ed organizzazione
Procedura Organizzativa	Uso della posta elettronica certificata e tradizionale
Procedura Organizzativa	Sottoscrizione documenti informatici
Procedura Organizzativa	Titolario di classificazione
Procedura Organizzativa	Amministratori di sistema
Istruzioni Operative	Formati elettronici dei documenti informatici
Istruzioni Operative	Elenco dei documenti esclusi dalla registrazione di protocollo
Istruzioni Operative	Descrizione del prodotto software di protocollo informatico in uso presso l’Ente
Istruzioni Operative	Abilitazioni all’utilizzo del sistema di gestione informatica dei documenti
Istruzioni Operative	Repertori generali
Istruzioni Operative	Politiche di sicurezza

Moduli	Lettera d'incarico al Custode Password Richiesta Password Comunicazione password

3. ASPETTI ORGANIZZATIVI PRELIMINARI (art. 5, comma 2, lettere a e i)

3.1 Individuazione Aree Organizzative Omogenee

L'art. 50, comma 4, del DPR 445/00 stabilisce che all'interno di ciascuna amministrazione siano create una o più Aree Organizzative Omogenee, in modo da assicurare criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna ad ognuna di esse.

L'art. 61 del DPR 445/00 stabilisce, altresì, che si costituisca per ciascuna AOO un Servizio responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al detto Servizio deve essere preposto un dirigente ovvero funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica.

L'art. 3 del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico" ribadisce l'obbligo di individuare le suddette Aree Organizzative Omogenee e di nominare, al loro interno, un Responsabile per la gestione documentale nonché un suo vicario per casi di vacanza, assenza o impedimento.

Questa amministrazione individua un'unica Area Organizzativa Omogenea denominata "***Comune di Arpaise***" che è composta dall'insieme di tutte le sue Unità Organizzative Responsabili (UOR), articolate come riportato nella **Procedura organizzativa** allegata "***Aree Organizzative Omogenee ed organizzazione***".

3.2 Accreditamento presso l'IPA

L'amministrazione/AOO si è dotata di una casella di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità dell'Ufficio incaricato della registrazione di protocollo.

Il medesimo ufficio procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

L'amministrazione, nell'ambito degli adempimenti previsti dall'art. 57-bis del CAD, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), tenuto e reso pubblico dall'Agenzia per l'Innovazione digitale (ex DigitPA).

Le informazioni inerenti l'Amministrazione e, nello specifico, comunicate all'IPA sono riportate nella Procedura Organizzativa allegata "Aree Organizzative Omogenee ed organizzazione".

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.

L'amministrazione, sempre ai sensi dell'art. 57-bis del D. Lgs. 7 marzo 2005, n. 82, comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire

l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'Amministrazione comunica la soppressione ovvero la creazione di una AOO.

3.3 Istituzione caselle di posta elettronica

Caselle di posta elettronica certificate

L'AOO del Comune è dotata di caselle di Posta Elettronica Certificata per la corrispondenza in ingresso ed in uscita, pubblicate sull'Indice delle Pubbliche Amministrazioni (IPA); una sola di esse è quella istituzionale, le altre sono caselle di struttura.

Tali caselle costituiscono l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento.

L'Allegato "***Uso della posta elettronica certificata e tradizionale***" descrive la procedura organizzativa per l'utilizzo delle caselle di posta elettronica assegnate all'interno dell'Ente.

Caselle di posta elettronica tradizionale

In attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione ha dotato i propri dipendenti di una casella di posta elettronica.

Nella Procedura Organizzativa "***Uso della posta elettronica certificata e tradizionale***" sono impartite le istruzioni per il corretto utilizzo delle caselle di posta elettronica tradizionale assegnate all'interno dell'Ente.

3.4 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici prodotti dall'Ente avviene in conformità a quanto previsto dal D. Lgs. 82/05 e dal DPCM 22/02/2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali".

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale ed archivistica, l'amministrazione fornisce la firma digitale e/o elettronica ai soggetti da essa delegati a rappresentarla.

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle suddette regole tecniche, garantisce l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento e, pertanto, ha l'efficacia della scrittura privata prevista dall'art. 2702 del Codice Civile.

La Procedura Organizzativa "*Sottoscrizione documenti informatici*" descrive in dettaglio le regole che l'Ente si è dato per l'uso delle sopra richiamate tipologie di firma e riporta i nominativi di coloro che all'interno dell'Ente, rivestendo specifici ruoli di responsabilità, sono titolari di firma digitale.

3.5 Istituzione del Servizio per la gestione documentale

Nell'ambito dell'Area Organizzativa Omogenea è istituito il ***Servizio per la gestione documentale***, ovvero per la "*tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi*", ai sensi dell'art. 61, comma 1, del Testo Unico.

L'ufficio preposto allo svolgimento delle attività afferenti al Servizio per la gestione documentale è denominato "**Ufficio Protocollo, Gestione documentale e Archivio"**.

A detto Ufficio sono ricondotti i compiti di cui all'articolo 61, comma 3 del DPR 28 dicembre 2000, n. 445, e all'art. 4 del D.P.C.M. 3/12/2013, ovvero:

- predisporre lo schema del Manuale di gestione documentale con la descrizione dei criteri e delle modalità di revisione del medesimo;
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico previsti dal Testo unico;
- predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare gli addetti dell'amministrazione all'utilizzo del software di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.);
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- garantire il buon funzionamento degli strumenti 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 operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

L'Ufficio "*Protocollo, Gestione documentale e Archivio*" costituisce, quindi, il servizio preposto alla gestione e tenuta dei documenti, prodotti o ricevuti dall'Ente nel corso dell'attività amministrativa. Ha competenza sull'intera documentazione archivistica, ovunque trattata, distribuita o conservata, ai fini della sua corretta classificazione, conservazione e ordinamento.

Il Responsabile del **Servizio per la gestione documentale** è la Dott.ssa Orsola Marra ed, in caso di vacanza, assenza o impedimento di quest'ultimo, la dott.ssa Daniela Donisi in qualità di suo Vicario.

In relazione alla protezione dei dati personali trattati al proprio interno l'Amministrazione ha ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento a:

- principio di necessità del trattamento dei dati;

- diritto di accesso ai dati personali da parte dell'interessato;
- modalità del trattamento e ai requisiti dei dati;
- informativa fornita agli interessati e relativo consenso se dovuto;
- nomina degli incaricati del trattamento;
- misure minime di sicurezza.

Regole e modalità operative stabilite dall'Amministrazione sono riportate nel piano di sicurezza di cui al capitolo 4.

3.6 Individuazione Unità Organizzative Responsabili e ruoli

Nell'allegato "Aree Organizzative Omogenee ed Organizzazione" è riportata la struttura organizzativa dell'Ente e sono descritti i ruoli delle figure responsabili individuate.

3.7 Adozione del Sistema di gestione informatica dei documenti

Per la gestione informatica dei documenti questa Amministrazione ha adottato la piattaforma applicativa della Società Halley.

Nell'allegato "*Descrizione del prodotto software di protocollo informatico in uso presso l'Ente*", in particolare, viene riportata la descrizione funzionale ed operativa del prodotto software di protocollo informatico in uso presso l'Ente.

Le informazioni riguardanti le "*Abilitazioni all'utilizzo del sistema di gestione informatica dei documenti*" sono riportate nelle Istruzioni Operative omonime, allegate al presente manuale.

3.8 Eliminazione dei protocolli di settore (art. 3, comma 1, lettera e)

Con l'entrata in funzione del sistema di gestione informatica dei documenti, sono eliminati tutti i sistemi di registrazione di protocollo alternativi al protocollo informatico.

3.9 Modello organizzativo adottato

Per la gestione dei documenti in entrata è adottato un modello di protocollazione di tipo centralizzato che prevede un unico ufficio per la protocollazione di tutti i documenti in ingresso.

Per la gestione dei documenti in uscita è adottato un modello di protocollazione di tipo decentrato che prevede la partecipazione attiva di più soggetti ed uffici utente.

Gli uffici utente ed i soggetti competenti per la ricezione, la registrazione, la classificazione e l'assegnazione dei documenti sono riportati nell'allegato "*Abilitazioni all'utilizzo del sistema di gestione informatica dei documenti*".

4. PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI (art. 5, comma 2, lettera b)

4.1 Scopo

Scopo del Piano di sicurezza è di garantire il rispetto delle misure minime di sicurezza, previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e succ. modd. e intt., relative alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici.

Esso è predisposto ai sensi dell'art. 5, comma 2, lettera b e dell'art. 4, comma 1, lettera c) del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013.

4.2 Obiettivo

Il piano di sicurezza garantisce che i documenti e le informazioni in esso contenuti siano trattati dall'Amministrazione/AOO nel rispetto dei principi di:

- **disponibilità** implementare tutte quelle azioni mirate a ridurre a un livello accettabile il rischio di non poter accedere ai dati da parte degli incaricati;
- **integrità** ridurre a un livello accettabile il rischio che i dati vengano alterati da persone non autorizzate;
- **riservatezza** ridurre a un livello accettabile il rischio che persone non autorizzate possano accedere ai dati.

Garantisce, inoltre, che i documenti contenenti dati personali comuni, sensibili e/o giudiziari 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.

4.3 Aspetti generali

Il piano di sicurezza è stato predisposto dal Responsabile del Servizio per la Gestione documentale in collaborazione con il Responsabile del Sistema Informatico, con il Responsabile del trattamento dei dati personali e con la collaborazione di personale esperto della società Halley.

Esso si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non) e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'Amministrazione, quindi, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato B del D.Lgs 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione periodica.

4.4 Definizione del piano ed articolazione dell'intervento

Il piano di sicurezza mette in evidenza l'esito delle attività di analisi preliminare, valutazione dei rischi e definizione delle politiche di sicurezza (misure adottate e da adottare) che riguardano tutti i Servizi dell'Ente interessati alla gestione documentale.

La definizione del piano di sicurezza richiede diverse azioni necessarie al raggiungimento dell'obiettivo che prevedono un intervento stratificato su più livelli:

- livello organizzativo
- livello logico
- livello fisico

Livello organizzativo

La messa in sicurezza a livello organizzativo viene attuata attraverso l'adozione di politiche, procedure organizzative, istruzioni operative, l'attuazione di norme, la pianificazione/erogazione di eventi formativi e/o informativi, l'assegnazione di ruoli e responsabilità, l'individuazione di scelte infrastrutturali che permettano di prevenire e ridurre i rischi che incombono sulla sicurezza dei documenti trattati con modalità informatiche.

Livello fisico

Mettere in sicurezza il patrimonio documentale digitale a livello fisico vuol dire adottare misure di sicurezza per il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico volte a limitare l'esposizione dell'Ente a rischi di incendio, furto, intrusione, allagamento e altre calamità.

Livello logico

La sicurezza a livello logico viene realizzata adottando una serie di misure per contrastare i rischi che incombono sull'infrastruttura telematica e tecnologica attraverso la quale avviene la gestione informatica del patrimonio documentale.

Nella figura seguente vengono schematizzate le fasi in cui è stato articolato l'intervento per la definizione del piano di sicurezza.

ARTICOLAZIONE DELL'INTERVENTO

Analisi preliminare

Dato il forte impatto trasversale che ha la sicurezza ed, in particolare, gli adempimenti previsti dal D. Lgs. 196/03 - Codice Privacy, è stato indispensabile procedere ad una azione di rilevazione e monitoraggio delle attività di trattamento svolte da ogni unità organizzativa dell'Ente al fine di avere un quadro generale e di verificare la compatibilità della situazione reale con le previsioni normative.

In questa fase è stata svolta una ricognizione presso l'Ente attraverso la rilevazione dettagliata di:

- struttura organizzativa (distribuzione di compiti e responsabilità),
- censimento dei trattamenti di documenti,
- rilevazione dei luoghi fisici afferenti all'Ente, dove avvengono i trattamenti e dove vengono conservati gli archivi documentali correnti e storici,
- rilevazione dell'infrastruttura hw, sw, di telecomunicazione e delle postazioni di lavoro informatiche,
- rilevazione delle applicazioni sw utilizzate per il trattamento dei documenti,
- rilevazione banche dati utilizzate.

L' Esito della fase di analisi è riportato nell'allegato "*Piano di Sicurezza*".

Valutazione dei rischi

A partire dalla definizione di una serie di eventi potenzialmente dannosi viene redatta l'analisi dei rischi incombenti sui dati, evidenziando la loro gravità in funzione del contesto riscontrato: fisico, logico, organizzativo.

L'analisi dei rischi è riportata nell'Allegato "Piano di Sicurezza".

Piano di adeguamento

Dalle attività precedenti scaturiscono una serie di considerazioni sulle misure di sicurezza già adottate o da adottare da parte dell'Ente, quindi, diviene possibile definire il piano di adeguamento da mettere in atto al fine di rendere sicuro e rispondente ai requisiti di legge l'intero sistema di gestione documentale dell'Ente.

Il piano di adeguamento (misure adottate e da adottare) per garantire la sicurezza dei dati è riportato nell'Allegato "*Piano di Sicurezza*".

Politiche di sicurezza

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

E' compito del Responsabile del Servizio per la Gestione documentale, in collaborazione con il Responsabile privacy e per la sicurezza informatica, procedere al perfezionamento, alla divulgazione, al riesame e alla verifica periodica delle politiche di sicurezza.

Le politiche di sicurezza stabilite sono riportate nelle Istruzioni Operative "*Politiche di Sicurezza*" allegate al presente Manuale.

Formazione del personale

In questa fase vengono programmate e pianificate le attività specifiche di formazione ed informazione per i responsabili e per gli incaricati del trattamento di documenti.

Il programma di formazione viene definito nell'Allegato "*Piano di formazione per il personale dell'Amministrazione".*

5. FORMAZIONE DEI DOCUMENTI (art. 5, comma 2, lettere c e d)

5.1 Disposizioni di carattere generale

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.

Prima di entrare nel merito, occorre caratterizzare l'oggetto della questione: il **documento amministrativo**.

Il documento amministrativo, in termini tecnologici, è classificabile in:

- **informatico**
- **analogico**

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- **ricevuto**
- **inviato**
- **interno formale**
- **interno informale**

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005

"*1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*"

e che

"*2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità*".

Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

5.2 Documento informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Ai sensi di quanto disposto dall'art. 20 del Codice dell'Amministrazione Digitale e dall'art. 3 del DPCM 13 novembre 2014, il documento informatico può essere formato mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi 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 informatica 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 basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

I formati elettronici utilizzati per la produzione dei documenti informatici, anche ai fini della conservazione rispettano le seguenti regole:

- sono conformi a quanto disposto dall'allegato 2 al DPCM 13 novembre 2014,
- sono aperti, completamente documentati e preferibilmente riconosciuti come standard da organismi internazionali,
- sono indipendenti da specifiche piattaforme tecnologiche hardware e software,
- non possono contenere macroistruzioni o codice eseguibile,
- sono ampiamente adottati,
- sono preferibilmente stabili e non soggetti a continue modificazioni nel tempo,
- sono preferibilmente utilizzabili con versioni precedenti e successive dell'applicativo software che li ha prodotti;
- sono privi di meccanismi tecnici di protezione che possano impedirne la replica del contenuto su nuovi supporti o la possibilità di effettuare migrazioni, pregiudicandone la fruibilità nel lungo periodo a causa dell'obsolescenza tecnologica;
- permettono la fruizione anche ad utenti diversamente abili.

I formati elettronici utilizzati dall'Ente sono quelli riportati nell'allegato "*Formati elettronici utilizzati*" del presente manuale.

5.3 Documento analogico - cartaceo

Per documento analogico si intende un documento amministrativo "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale".

Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampata.

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

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del Manuale.

5.4 Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato:

1. a mezzo posta elettronica convenzionale o certificata;
2. su supporto rimovibile quale, ad esempio, CD ROM, DVD, floppy disk, tape, pen drive, etc, consegnato direttamente all'Ufficio "*Protocollo, Gestione documentale e Archivio"* o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telegramma;
4. con consegna a mano da parte dell'interessato o di altra persona dallo stesso delegata all'Ufficio "*Protocollo, Gestione Documentale e Archivio"* e/o agli Uffici Organizzativi di Riferimento aperti al pubblico.

5.5 Documento inviato

Un **documento informatico**, compreso di eventuali allegati, anch'essi informatici, è inviato, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.

In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso al destinatario con mezzi di trasposto non telematici, tradizionalmente utilizzati per inviare documenti analogici, come descritti nel successivo paragrafo.

Un documento analogico può essere inviato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telegramma;
4. mediante consegna a mano da parte di un messo notificatore delegato dall'Ente.

5.6 Documento interno formale

I documenti interni sono formati con tecnologie informatiche.

Lo scambio di documenti informatici di rilevanza amministrativa giuridico probatoria tra Uffici Organizzativi di Riferimento interni all'Ente, avviene di norma attraverso i seguenti mezzi:

- sistema di messaggistica interna (se disponibile)
- posta elettronica convenzionale
- posta elettronica certificata

Il documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato.

Il sistema di messaggistica interna adottato dall'Amministrazione è quello fornito dalla Società Halley.

Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con

strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato.

5.7 Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

Per la formazione, la gestione e la sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna AOO può adottare, nella propria autonomia organizzativa regole diverse da quelle contenute nelle regole tecniche vigenti. In questa eventualità, le diverse regole adottate saranno pubblicate nel presente Manuale.

5.8 Contenuti minimi

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.

Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale:

- tratta un unico argomento, indicato dall'autore, in maniera sintetica ma esaustiva nello spazio riservato all'oggetto;
- è riferito ad un solo protocollo;
- può far riferimento a più fascicoli.

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli uffici organizzativi di riferimento.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'ufficio organizzativi di riferimento che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono dell'ufficio organizzativi di riferimento;
- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del Responsabile del Procedimento Amministrativo e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo e/o del responsabile del provvedimento finale.

- 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 moduli e formulari elettronici validi ad ogni effetto di legge.

5.9 Sottoscrizione di documenti informatici

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

L'amministrazione, quando non si configura come autorità di certificazione, si avvale dei servizi di una autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'AGID.

I documenti informatici prodotti dall'amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità e la leggibilità nel tempo. A tal proposito, l'art. 4 comma 3 del decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 asserisce che un documento non soddisfa il requisito dell'immodificabilità se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Nell'Allegato "*Sottoscrizione documenti informatici*" viene riportato l'elenco del documenti prodotti dalla AOO, soggetti o meno alla sottoscrizione digitale, distinti anche per tipologia di sottoscrizione.

6. GESTIONE CORRISPONDENZA IN ENTRATA (art. 5, comma 2, lett. f, g e h)

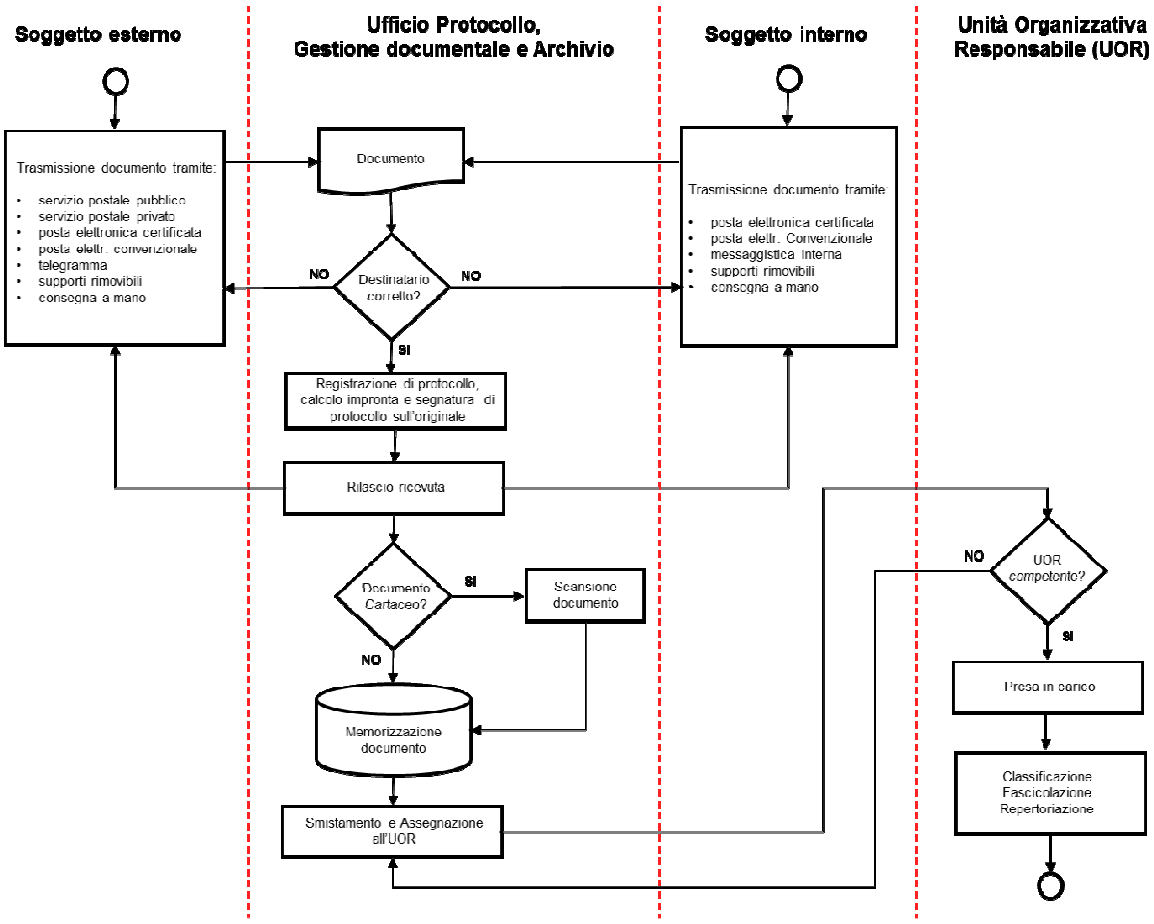
Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti dalla AOO dell'Ente.

6.1 Flusso dei documenti ricevuti dalla AOO

Nello schema grafico che segue è rappresentato il flusso risultante dall'attività di reingegnerizzazione dei processi dell'Ente, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno dell'Ente stesso.

La modalità di rappresentazione grafica utilizzata consente di disegnare il flusso del processo evidenziando:

- gli attori del processo
- le eventuali fasi del processo
- le attività in cui il processo si articola
- il flusso delle attività
- gli input e gli output delle attività stesse



Nei paragrafi seguenti viene descritto il processo sopra rappresentato graficamente.

6.2 Ricezione

Un documento può pervenire all'**Ufficio "*Protocollo, Gestione documentale e Archivio*"** dell'Ente da parte di un soggetto esterno all'Amministrazione, attraverso i seguenti mezzi:

- posta convenzionale (servizio postale pubblico o privato)
- posta elettronica certificata
- posta elettronica convenzionale
- telegramma
- supporto rimovibile
- consegna a mano

Un documento può pervenire all' **Ufficio "*Protocollo, Gestione documentale e Archivio*"**dell'Ente anche da parte di un soggetto interno all'Amministrazione stessa; in questo caso i mezzi attraverso cui può avvenire la trasmissione possono essere:

- posta elettronica certificata
- posta elettronica convenzionale
- supporto rimovibile
- consegna a mano

6.2.1 Ricezione a mezzo posta convenzionale (servizio postale pubblico o privato)

I documenti che transitano attraverso il servizio postale pubblico sono ritirati quotidianamente secondo le regole stabilite dal Responsabile per la "*Gestione documentale*".

Quelli che arrivano attraverso servizio postale privato vengono consegnati dal corriere privato all'**Ufficio "*Protocollo, Gestione documentale e Archivio*"**dell'Ente.

Le buste o contenitori vengono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario apposti sugli stessi.

Per tutta la corrispondenza non rientrante nelle categorie specifiche di seguito indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

Corrispondenza relativa ai bandi di gara

La corrispondenza relativa ai bandi di gara viene registrata al protocollo e successivamente consegnata chiusa all'ufficio responsabile della gara.

Corrispondenza personale

La corrispondenza personale non deve essere aperta, né protocollata ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo per la registrazione.

Ricevute di ritorno della posta raccomandata

Le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo con le modalità descritte nel successivo capitolo.

6.2.2 Ricezione attraverso la casella di PEC istituzionale

La ricezione dei documenti informatici è assicurata tramite la casella di Posta Elettronica Certificata (PEC) istituzionale che è gestita dall'Ufficio "*Protocollo, Gestione documentale e Archivio*".

Ogni documento che arriva attraverso la casella di PEC istituzionale viene preso in carico dall'Ufficio "*Protocollo, Gestione documentale e Archivio*" che provvede alla sua registrazione di protocollo, previa verifica della correttezza del destinatario, della validità della firma apposta e della leggibilità del documento.

Nel caso in cui il documento sia pervenuto per errore in quanto indirizzato ad altro destinatario, lo stesso viene restituito al mittente con la dicitura "Messaggio pervenuto per errore non di competenza di questa AOO".

Ulteriori dettagli sulle modalità di utilizzo della casella di PEC istituzionale sono riportati nell'Allegato "*Istruzioni operative sull'uso della posta elettronica certificata e tradizionale*".

6.2.3 Ricezione attraverso caselle di posta elettronica non istituzionali

Un messaggio ricevuto su una casella di posta elettronica non istituzionale viene preso in carico dal Responsabile del procedimento amministrativo che valuta se il messaggio debba essere protocollato, nel qual caso viene inoltrato alla casella di PEC istituzionale per la relativa registrazione di protocollo.

Le istruzioni operative di dettaglio sono riportate Allegato "*Istruzioni operative sull'uso della posta elettronica certificata e tradizionale*".

6.2.4 Ricezione su supporti rimovibili

Un documento digitale può essere consegnato all'AOO su supporto di memoria rimovibile.

Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a propria disposizione.

Il documento ricevuto nella forma de quò viene sottoposto a tutti i controlli specifici, superati i quali viene registrato al protocollo ed inserito nel flusso di lavorazione.

6.2.5 Ricezione corrispondenza tramite telegramma o via telefax

La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, viene trattata come un documento cartaceo con le modalità descritte nel successivo capitolo.

L'uso del telefax non è più consentito. In seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto 2013, l'art. 14 ha stabilito, infatti, che ai fini della verifica della provenienza delle comunicazioni è in ogni caso esclusa la trasmissione di documenti a mezzo fax.

6.2.6 Ricezione tramite consegna a mano

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente. In questo caso viene rilasciata al mittente o al suo delegato ricevuta senza gli estremi del protocollo.

6.3 Errata ricezione

Documenti informatici

Nel caso in cui pervengano all'Ente/AOO messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente con la seguente dicitura:

"*Messaggio pervenuto per errore - non di competenza di questo/a Ente/AOO*".

Documenti cartacei

Nel caso in cui pervengano erroneamente all'Ufficio "Protocollo, Gestione documentale e Archivio" dell'Amministrazione documenti indirizzati ad altri soggetti, questo Ufficio provvede alla restituzione della corrispondenza alla posta.

Qualora la busta fosse aperta per errore, il documento va protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "*documento pervenuto per errore*" e si invia al mittente apponendo sulla busta la dicitura "*Pervenuta ed aperta per errore*".

6.4 Rilascio di ricevute attestanti la ricezione

Documenti informatici

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Il sistema di protocollazione informatica dei documenti provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- messaggio di conferma di protocollazione: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;
- messaggio di notifica di eccezione: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza.
- messaggio di aggiornamento di protocollazione: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

Documenti cartacei

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all'Ufficio "*Protocollo, Gestione documentale e Archivio*" ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'Ufficio è autorizzato a:

- fotocopiare gratuitamente la prima pagina del documento;
- se contestualmente alla ricezione avviene anche la protocollazione
  - apporre gli estremi della segnatura;
  - altrimenti, apporre sulla copia così realizzata il timbro dell'amministrazione con la data e l'ora d'arrivo e la sigla dell'operatore.

6.5 Tutela della privacy relativa ai documenti cartacei ricevuti a mezzo posta convenzionale

Se per errore la corrispondenza viene recapitata ad un ufficio diverso dall'Ufficio "Protocollo, Gestione documentale e Archivio", a tutela dei dati personali eventualmente contenuti nella missiva, l'Ufficio ricevente non apre la busta, ma rilascia ricevuta al mittente nelle forme stabilite dal Responsabile per la "*Gestione documentale*", quindi, invia nella stessa giornata e prima della chiusura, la posta all'Ufficio "Protocollo, Gestione documentale e Archivio" che è abilitato e incaricato dell'apertura della corrispondenza e della protocollazione.

6.6 Registrazione di protocollo e segnatura

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e "segnati" nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliati nel successivo capitolo.

6.7 Archiviazione

Documenti informatici

I documenti informatici vengono archiviati nel repository documentale, attraverso il software applicativo di gestione del protocollo informatico, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

I documenti ricevuti per via telematica, subito dopo l'operazione di smistamento e di assegnazione, vengono resi disponibili agli Uffici destinatari attraverso il sistema di protocollo informatico accessibile dagli utenti autorizzati e collegati alla rete interna dell'amministrazione/AOO.

Documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, vengono acquisiti in formato immagine attraverso un processo di scansione, utilizzando l'applicazione sw di gestione del protocollo informatico.

Il processo di scansione avviene come segue:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento delle immagini alle rispettive registrazioni di protocollo in modo non modificabile;
- memorizzazione delle immagini su supporto informatico, in modo non modificabile.

Le rappresentazioni digitali dei documenti cartacei sono archiviate, secondo le regole vigenti, nel repository documentale, in modo non modificabile al termine del processo di scansione.

I documenti cartacei, dopo l'operazione di riproduzione in formato immagine, vengono inviati agli Uffici destinatari per le successive operazioni di fascicolazione e conservazione.

I documenti con più destinatari, dopo la riproduzione in formato immagine, vengono inviati a tutti in formato elettronico. <opzionale: Il documento cartaceo originale viene inviato solo al primo destinatario>.

La riproduzione dei documenti cartacei in formato immagine viene eseguita sulla base dei seguenti criteri:

- se il documento ricevuto in formato A4 o A3 non supera le poche pagine viene acquisito direttamente con le risorse, umane e strumentali, interne all'AOO;
- se il documento ha una consistenza maggiore o formati diversi dai precedenti, viene acquisito in formato immagine solo se esplicitamente richiesto dagli Uffici di competenza dei procedimenti, avvalendosi eventualmente dei servizi di una struttura esterna specializzata.

In questo caso il Responsabile per la Gestione Documentale individua i documenti da sottoporre al processo di scansione e ne fissa i tempi, diversi da quelli ordinari, e le modalità esecutive.

In ogni caso non vengono riprodotti in formato immagine le seguenti tipologie di documenti:

- certificati medici contenenti la diagnosi,

L'Ufficio "Protocollo, Gestione documentale e Archivio" è abilitato all'operazione di scansione dei documenti.

6.8 Classificazione, smistamento, assegnazione e presa in carico

L'attività di smistamento consiste nell'operazione di inviare un documento protocollato e segnato all'Unità Organizzativa Responsabile competente in base alla classificazione di primo livello del titolario, effettuata per il documento.

Con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione.

Effettuata, quindi, la classificazione di primo livello, lo smistamento e l'assegnazione, il Responsabile del Procedimento Amministrativo provvede alla presa in carico del documento che gli è stato assegnato.

Una volta che al mittente iniziale (Unità Organizzativa di Protocollo) giunge notizia di presa in carico della corrispondenza, è cura di quest'ultimo consegnare, con le tecnologie idonee, il documento oggetto di lavorazione compilato nella parte di segnatura (o timbro di segnatura) all'Unità Organizzativa Responsabile o al Responsabile del Procedimento Amministrativo di competenza.

L'assegnazione può essere effettuata per conoscenza o per competenza.

L'Unità Organizzativa Responsabile competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.

I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

Nell'Allegato "Procedura Organizzativa – Aree Organizzative Omogenee e Organizzazione" sono riportate le Unità Organizzative Responsabili che possono essere destinatarie dello smistamento da parte dell'Ufficio "*Protocollo, Gestione Documentale e Archivio*".

alternativa 1

Il personale addetto all'Ufficio "*Protocollo, Gestione documentale e Archivio*" esegue, attraverso il software di gestione protocollo informatico, la classificazione di primo livello del documento sulla base del titolario di classificazione adottato dall'Amministrazione/AOO e provvede ad inviarlo all'Ufficio di destinazione che, a sua volta:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, il documento è ritrasmesso all'Ufficio "*Protocollo, Gestione documentale e Archivio*";
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandolo al proprio interno al Responsabile del procedimento o ad altro utente incaricato dell'espletamento della pratica.

alternativa 2

Il personale addetto all'Ufficio "Protocollo, Gestione documentale e Archivio" provvede ad inviare il documento all'ufficio di destinazione. Quest'ultimo:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore rinvia il documento all'ufficio "Protocollo, Gestione documentale e Archivio";
- in caso di verifica positiva, esegue, attraverso il software di gestione protocollo informatico, la classificazione di primo livello del documento sulla base del titolario di classificazione adottato dall'Amministrazione/AOO e provvede a smistarlo al proprio interno al Responsabile del procedimento o ad altro utente incaricato dell'espletamento della pratica.

6.9 Fascicolazione e conservazione dei documenti nell'archivio corrente

L'ultima fase del flusso di lavorazione della corrispondenza in ingresso prevede le seguenti attività:

- classificazione di livello superiore sulla base del titolario di classificazione adottato dall'AOO;
- fascicolazione del documento secondo le procedure previste dall'AOO;
- nel caso di apertura di un nuovo fascicolo, inserimento del fascicolo nel repertorio dei fascicoli.

Responsabili dell'organizzazione, della tenuta dei fascicoli in fase attiva (prima del riversamento nell'archivio di deposito) e della conservazione dei documenti al loro interno sono i Responsabili dei procedimenti.

7. REGISTRAZIONE DEI DOCUMENTI (art. 5, comma 2, lettera e, j, k, n, q)

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

7.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica, indipendentemente dal modello organizzativo adottato dall'AOO medesima, centralizzato o distribuito delle unità organizzative di registrazione del 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 almeno 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 unità organizzativa di protocollo viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

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

7.2 Registrazione di protocollo

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

Su 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, registrato in forma non modificabile;
- il destinatario del documento, registrato in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la classificazione.

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

Tali dati facoltativi sono descritti nei paragrafi seguenti.

7.2.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'amministrazione.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne abbia accertato l'autenticità, la provenienza, l'integrità ed abbia verificato la validità della firma.

Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

L'Ufficio "*Protocollo, Gestione documentale e Archivio*" riceve i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

7.2.2 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, ovvero attraverso il servizio postale pubblico e/o privato o con consegna diretta all'Ufficio "*Protocollo, Gestione documentale e Archivio*".

La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'Amministrazione/AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita o interna formale, l'Ufficio "*Protocollo, Gestione documentale e Archivio*" esegue la registrazione di protocollo dopo che il documento abbia superato tutti i controlli formali sopra richiamati.

7.2.3 Elementi facoltativi della Registrazione di protocollo

Il Responsabile per la "*Gestione documentale*", con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo.

La registrazione degli elementi facoltativi del protocollo, con determinazione del Responsabile per la "*Gestione documentale*" può essere modificata, integrata e cancellata in base alle effettive esigenze delle unità organizzative o degli uffici.

I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- ora e minuto di registrazione;
- luogo di provenienza o di destinazione del documento;
- tipo di documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, ecc.);
- collegamento a documenti precedenti e susseguenti;
- numero degli allegati;
- riferimenti agli allegati su supporto informatico;
- nominativo dei destinatari delle copie per conoscenza;
- unità organizzativa/ufficio competente;
- identificativo del Responsabile del procedimento amministrativo;
- termine di conclusione del procedimento amministrativo o di lavorazione del documento;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- stato e tempi parziali delle procedure del procedimento amministrativo;
- classificazione del documento (titolo, categoria e fascicolo; eventuale sottofascicolo e inserto);
- data di istruzione del fascicolo;

- numero del fascicolo;
- numero del sottofascicolo;
- numero dell'inserto;
- data di chiusura del fascicolo;
- repertorio dei fascicoli;
- identificativo del fascicolo e/o del documento;
- numero di repertorio della serie (delibere, determinazioni, verbali, circolari e contratti);
- tipologia del documento con l'indicazione dei termini di conservazione e di scarto;
- scadenzario.

7.3 Segnatura di protocollo

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.

7.3.1 Segnatura documenti informatici

Ai sensi degli artt. 9 e 21 del D.P.C.M. 3/12/2013, le informazioni minime incluse nella segnatura di protocollo dei documenti informatici, registrati nel registro di protocollo e negli altri registri riferiti all'art. 53, comma 5, del D.P.R. 28-12-2000, n. 445 (altrimenti detto "Testo Unico"), sono quelle di seguito elencate:

a) codice identificativo dell'Amministrazione;
b) codice identificativo dell'Area Organizzativa Omogenea;
c) codice identificativo del registro;
d) data di protocollo secondo il formato individuato in base alle previsioni di cui all'art. 20, comma 2 del D.P.C.M. 03/12/2013
e) progressivo di protocollo secondo il formato specificato all'art. 57 del già citato Testo Unico;
f) oggetto;
g) mittente;
h) destinatario/i.

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) definito e aggiornato periodicamente dall'Agenzia per l'Italia Digitale con provvedimento reso disponibile sul proprio sito (D.P.C.M. 3/12/2013, art. 20).

Nella segnatura di un documento protocollato in uscita possono essere specificate le seguenti altre informazioni, incluse anch'esse nello stesso file, (art. 21, D.P.C.M. 3/12/2013)

- indicazione della persona o dell'ufficio all'interno della struttura destinataria;
- indice di classificazione;
- identificazione degli allegati;

- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.

E' possibile aggiungere alla segnatura eventuali altre informazioni che due o più amministrazioni stabiliscano, di comune accordo, di scambiarsi a condizione che vengano rispettate le indicazioni tecniche stabilite dall'Agenzia per l'Italia Digitale.

7.3.2 Segnatura documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo dell'amministrazione,
- codice identificativo dell'AOO;
- data e numero di protocollo del documento;

Facoltativamente, possono essere riportate anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il codice identificativo dell'unità organizzativa di riferimento a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo;
- ogni altra informazione utile o necessaria, se già disponibile al momento della registrazione di protocollo.

Il "segno" grafico di norma è realizzato con una etichetta autoadesiva corredata di codice a barre o, in alternativa, con un timbro tradizionale.

L'operazione di segnatura dei documenti in partenza viene effettuata dall'Unità organizzativa competente che redige il documento se è abilitata alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dall'Ufficio "*Protocollo, Gestione documentale e Archivio*".

L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo deve essere apposto sulla prima pagina dell'originale; in caso contrario il "segno" viene apposto sul retro della prima pagina dell'originale.

7.4 Riservatezza delle registrazioni di protocollo

Le registrazioni di protocollo, la segnatura, la registrazione delle informazioni annullate o modificate avvengono attraverso il sistema di protocollo informatico che garantisce la protezione di tali informazioni attraverso l'adozione delle misure di sicurezza ampiamente descritte nel capitolo 4 "piano di sicurezza", tra cui quelle che riguardano il controllo degli accessi e i livelli di autorizzazione previsti.

7.5 Immodificabilità e annullamento registrazioni di protocollo (art. 5, comma 2, lettera n)

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile, per correggere errori verificatisi in sede

di immissione manuale di dati, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile per la "*Gestione documentale*".

In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

Solo il Responsabile per la "*Gestione documentale*" è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile per la "*Gestione documentale*".

A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.

Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

7.6 Registro giornaliero di protocollo (art. 5, comma 2, lettera n)

Il Responsabile del Servizio per la gestione documentale provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, ai sensi dell'art. 7, comma 5, del DPCM 3/12/2013, il registro giornaliero informatico di protocollo è trasmesso al sistema di conservazione entro la giornata lavorativa successiva.

Tale operazione di riversamento viene espletata adottando le regole tecniche in materia di conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi del DPCM del 13/11/2014.

7.7 Registro di emergenza (art. 5, comma 2, lettera q)

Il responsabile per la "Gestione documentale" autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo sul registro di emergenza ogni volta che per cause tecniche non sia possibile utilizzare il sistema informatico di protocollo, come stabilito dall'art. 63 del Testo Unico sulla documentazione amministrativa.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno. Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il Responsabile per la Gestione Documentale annota sullo stesso il mancato uso.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

Per semplificare la procedura di apertura del registro di emergenza Il sistema di protocollo informatico adottato dall'Amministrazione permette di scaricare un modello del registro di

emergenza in cui inserire i dati da una postazione fuori linea fino al momento in cui non viene ristabilito il funzionamento del protocollo informatico.

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

Quando l'impossibilità si prolunghi per oltre 24 ore, il Responsabile per la "Gestione documentale" può autorizzare l'uso del registro di emergenza per un periodo successivo di non più di una settimana riportando sul registro gli estremi del provvedimento di autorizzazione.

Per ogni giornata di registrazione di emergenza è riportato il numero delle operazioni registrate manualmente.

Appena il sistema informatico viene riattivato, vanno inserite le informazioni relative ai documenti protocollati in emergenza, utilizzando un'apposita funzione di recupero dei dati.

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 è associato 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 del procedimento amministrativo.

Sino al completo inserimento dei dati è inibito di procedere a nuove protocollazioni.

In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo

Una volta ripristinata la piena funzionalità del Sistema informatico di protocollo, il Responsabile del Servizio per la "Gestione documentale" provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

7.8 Differimento dei termini di registrazione

Le registrazioni di protocollo dei documenti pervenuti presso l'Amministrazione sono effettuate nella giornata di arrivo e, comunque, non oltre le 48 ore dal ricevimento di detti documenti.

Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del Responsabile per la "*Gestione documentale*", che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.

Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il Responsabile per la "*Gestione documentale*" descrive nel provvedimento sopra citato.

7.9 Elenco dei documenti esclusi dalla registrazione di protocollo (art. 5, comma 2, lettera j)

Nelle Istruzioni Operative "*Documenti esclusi dalla registrazione di protocollo e soggetti a registrazione particolare*" si riporta l'elenco delle tipologie di documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 53, comma 5 del Testo Unico.

7.10 Casi particolari di registrazioni di protocollo

7.10.1 Documenti soggetti a registrazioni particolari

All'interno dell'AOO è istituito il protocollo riservato, sottratto alla consultazione da parte di chi non sia espressamente abilitato, nel quale sono riportati:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente richiamati nelle Istruzioni Operative "*Documenti esclusi dalla registrazione di protocollo e soggetti a registrazione particolare*".

La registrazione nel protocollo particolare, quando non sia palesemente evidente la necessità, può essere disposta dal Responsabile per la "*Gestione documentale*" con l'apposizione, sul documento, della seguente dicitura: "Da registrare sul protocollo particolare".

I documenti (informatici o cartacei) anonimi, come tali individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale, vengono inviati al Responsabile per la "*Gestione documentale*" che ne effettua una valutazione:

- se ritiene che contengano dati o informazioni di interesse dell'amministrazione/AOO, provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni. Questi decidono se farli registrare nel protocollo generale;
- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo particolare.

Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

Sui documenti appartenenti a questa categoria vanno eseguite tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.

Questi documenti costituiscono comunque delle serie d'interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

- dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, data di adozione, oggetto….);
- numero di repertorio (numero progressivo);
- dati di classificazione e di fascicolazione.

7.10.2 Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.

I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

7.10.3 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale con la dicitura “Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari - Vedi elenco allegato alla minuta/copia presso l’Unità organizzativa di riferimento”.

Tale elenco, in formato cartaceo, viene allegato alla minuta dell’originale.

7.10.4 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al servizio protocollo come documenti senza firma specificando tale modalità di trasmissione nel sistema di protocollo informatico.

7.10.5 Protocollazione di un numero consistente di documenti cartacei

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

7.10.6 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dall’interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell’avvenuta consegna con gli estremi della segnatura di protocollo.

Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.

Nell’eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente, come descritto nel paragrafo 7.8. In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

7.10.7 Fatture, assegni e altri valori di debito e credito

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall’altra posta in arrivo, protocollate su un registro diverso da quello generale e inviate quotidianamente all’unità organizzativa responsabile competente.

7.10.8 Protocollazione di documenti inerenti a gare di appalto confezionati su supporti cartacei

La corrispondenza che riporta l’indicazione “offerta” - “gara d’appalto” - “preventivo” o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l’apposizione della segnatura, della data, dell’ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all’unità organizzativa responsabile competente.

È compito della stessa unità organizzativa responsabile provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

Dopo l'apertura delle buste l'unità organizzativa responsabile che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

Per motivi organizzativi tutte le unità organizzative responsabili sono tenute ad informare preventivamente il Responsabile per la "*Gestione documentale*" in merito alle scadenze di concorsi, gare, bandi di ogni genere.

7.10.9 Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.

Solo in questo caso il Responsabile per la "*Gestione documentale*" si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo pervenuto o da spedire.

Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'Ufficio "*Protocollo, Gestione documentale e Archivio*".

7.10.10 Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal Responsabile del servizio per la "*Gestione documentale*" attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

È poi compito dell'unità organizzativa di competenza e, in particolare, del Responsabile del procedimento amministrativo valutare se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

7.10.11 Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via telegramma, fermo restando che il Responsabile del procedimento amministrativo deve verificare la provenienza certa del documento; in caso di mittente non verificabile, il Responsabile del procedimento amministrativo valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;

- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

Ad ogni modo, se il Responsabile del Procedimento valuta l'opportunità di protocollare la missiva procede, come descritto nel par. 6.2.3, all'inoltro del messaggio alla casella di P.E.C. istituzionale per la relativa registrazione di protocollo.

7.10.12 Copie per conoscenza

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 7.10.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.

Tale informazione è riportata anche sulla segnatura di protocollo.

7.10.13 Registrazioni di documenti temporaneamente riservati

Quando si è in presenza di documenti che per la loro natura richiedono una temporanea riservatezza delle informazioni in essi contenute (ad esempio gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso riservato al protocollo generale.

Il responsabile dell'immissione dei dati provvede alla registrazione di protocollo indicando contestualmente l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate saranno accessibili nelle forme ordinarie.

7.10.14 Corrispondenza personale o riservata

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "*riservata*" o "*personale*".

In quest'ultimo caso, la corrispondenza con la dicitura "*riservata*" o "*personale*" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

7.11 Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

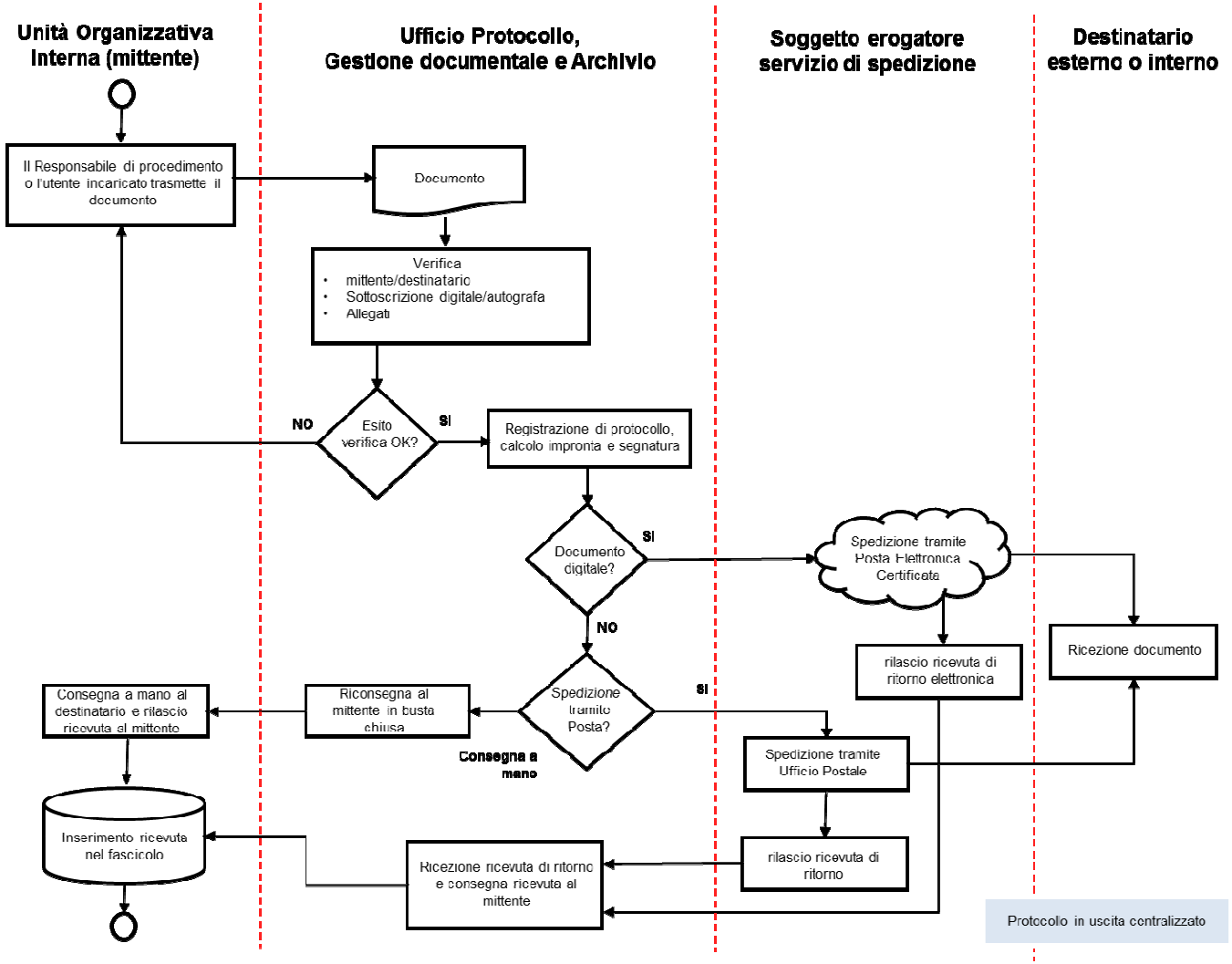
I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

8. GESTIONE CORRISPONDENZA IN USCITA (art. 5, comma 2, lettera f)

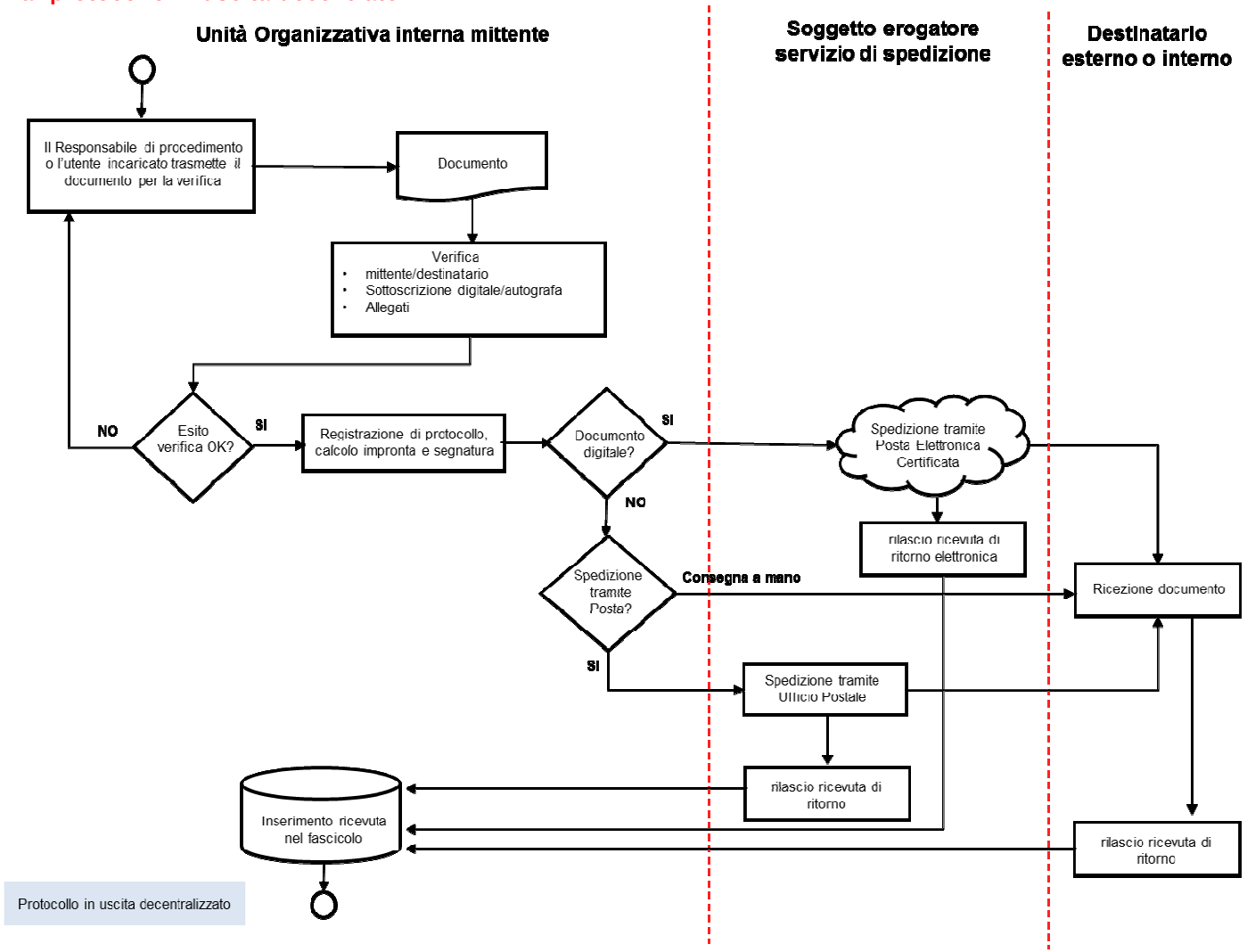
8.1 Flusso dei documenti inviati dalla AOO

Seguono due rappresentazioni grafiche del flusso di lavoro per i documenti in uscita, a seconda che l'Amministrazione adotti un modello centralizzato per la gestione del protocollo informatico (la protocollazione è affidata solo all'Ufficio "Protocollo, Gestione documentale e Archivi") oppure un modello Decentrato (ogni Unità organizzativa si occupa in autonomia della registrazione di protocollo dei documenti in uscita di propria competenza).

Prima alternativa: protocollo in uscita centralizzato



Seconda alternativa: protocollo in uscita decentrato



8.2 Invio documento da parte del soggetto interno mittente

Per soggetto interno mittente si intende l'unità organizzativa interna all'AOO da cui ha origine il documento da inviare al destinatario che può essere un'altra Amministrazione oppure un'altra AOO della stessa Amministrazione o, ancora, un altro ufficio della stessa AOO.

Il documento in partenza viene prodotto dal personale degli uffici dell'AOO mittente nell'esercizio delle proprie funzioni, ha rilevanza giuridico-probatoria ed è destinato ad essere trasmesso ad un soggetto destinatario tra quelli appena citati.

Il documento da spedire può essere predisposto:

- in formato digitale, formato secondo gli standard illustrati nei precedenti capitoli;
- in formato analogico, durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale.

Il documento in formato digitale può essere trasmesso attraverso la posta elettronica certificata. Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente) su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.

Il documento in formato analogico può essere recapitato tramite il servizio postale, nelle sue diverse forme, oppure attraverso consegna a mano.

8.3 Verifica formale del documento in partenza

La procedura si differenzia a seconda che l'Amministrazione adotti un modello centralizzato o Decentrato per la gestione del protocollo informatico.

< Modello Centralizzato >

I documenti originali da spedire vengono inoltrati all'Ufficio "*Protocollo, Gestione documentale e Archivio*".

Se i documenti sono in formato digitale vengono inviati alla casella di posta interna dedicata alla funzione di "appoggio" per i documenti digitali da spedire.

Se i documenti sono in formato analogico vengono consegnati in busta aperta per le operazioni successive di protocollazione e segnatura. Possono essere consegnati in questa forma anche i documenti contenenti i dati personali sensibili o giudiziari in quanto il personale dell'Ufficio "Protocollo, Gestione documentale e Archivio", è autorizzato al trattamento dei dati personali.

L'Ufficio "*Protocollo, Gestione documentale e Archivio*", provvede ad eseguire le verifiche di conformità della documentazione ricevuta, cioè verifica che siano indicati correttamente il mittente e il destinatario, verifica che il documento sia sottoscritto in modalità digitale o autografa, la presenza di allegati se dichiarati.

Se il documento è completo, esso è registrato nel protocollo generale o particolare e ad esso viene apposta la segnatura in base alla tipologia di documentazione da inviare; in caso contrario è rispedito al mittente con le osservazioni del caso.

< Modello Decentrato >

Ogni Unità Organizzativa Responsabile è autorizzata dall'AOO, per il tramite del Responsabile di Procedimento, a svolgere attività di registrazione di protocollo e

apposizione della segnatura per la corrispondenza in uscita, attraverso l'applicazione di protocollo informatico adottata dall'Ente.

Di conseguenza le unità organizzative responsabili provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo generale o particolare e, quindi spedito; in caso contrario è restituito al mittente con le osservazioni del caso.

8.4 Registrazione di protocollo e segnatura del documento in partenza

La procedura si differenzia a seconda che l'Amministrazione adotti un modello centralizzato o Decentrato per la gestione del protocollo informatico.

< Modello Centralizzato >

Le operazioni di registrazione e di apposizione della segnatura del documento in partenza sono effettuate presso l'Ufficio "*Protocollo, Gestione documentale e Archivio*".

In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili.

La compilazione di moduli se prevista (ad es. nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere) è a cura dell'Unità Organizzativa interna mittente.

< Modello Decentrato >

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dell'Unità Organizzativa interna mittente, abilitata ad accedere al sistema di protocollo informatico dell'AOO a cui appartiene.

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

8.5 Spedizione del documento informatico

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AGID del 23 gennaio 2013, n. 60.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).

Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dall'Agenzia per l'Italia Digitale. Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.

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, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei 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.

8.6 Spedizione del documento analogico

La procedura si differenzia a seconda che l'Amministrazione adotti un modello centralizzato o Decentrato per la gestione del protocollo informatico.

< Modello Centralizzato >

L'Ufficio "*Protocollo, Gestione documentale e Archivio*" provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici

(Opzionalmente: I documenti da spedire su supporto cartaceo, nell'ambito dell'Ufficio "*Protocollo, Gestione documentale e Archivio*", sono trasmessi all'ufficio addetto allo smistamento della posta, se previsto, abilitato alla spedizione "fisica" della corrispondenza).

L' Ufficio "*Protocollo, Gestione documentale e Archivio*" conserva, temporaneamente, la minuta da restituire al mittente.

< Modello Decentrato >

L'Unità Organizzativa mittente provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.

(Opzionalmente: I documenti da spedire su supporto cartaceo, nell'ambito della AOO, sono trasmessi all'ufficio addetto allo smistamento della posta, se previsto, abilitato alla spedizione "fisica" della corrispondenza).

In entrambi i casi, qualora i destinatari siano più di uno, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

L'Ufficio Protocollo effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

8.7 Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.

< Modello Centralizzato >

L'Ufficio "*Protocollo, Gestione documentale e Archivio*" che effettua la spedizione centralizzata di documenti informatici o cartacei cura anche l'invio delle ricevute di ritorno al mittente che si fa carico di archiviarle nel fascicolo logico o fisico.

< Modello Decentrato >

L'Unità Organizzativa Interna mittente, che effettua la spedizione di documenti informatici o cartacei direttamente, cura anche l'archiviazione delle ricevute di ritorno.

9. GESTIONE DEI DOCUMENTI INTERNI, DEI FLUSSI DOCUMENTALI E DEI PROCEDIMENTI AMMINISTRATIVI (art. 5, comma 2, lettera f)

Le fasi della gestione dei documenti interni all'AOO/Amministrazione sono le seguenti:

1. formazione (le regole sono descritte nel cap. 5);
2. registrazione e segnatura di protocollo, necessaria solo nei casi in cui si renda necessario definirne la data certa (le regole sono descritte nel cap. 7)
3. classificazione (le regole sono descritte nel par. 6.8 e nel cap. 12);
4. fascicolazione (le regole sono descritte nel cap.12).

9.1 Gestione dei flussi documentali tra gli uffici dell'AOO

I flussi di lavorazione dei documenti all'interno dell'AOO fanno riferimento ai diagrammi riportati nei capitoli 6 e 8 ed ivi descritti.

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

- ricevuti dall'Amministrazione/AOO, dall'esterno o anche dall'interno e destinati ad essere ritrasmessi/assegnati in modo formale in seno all'AOO;
- inviati dall'Amministrazione all'esterno o anche all'interno dell'AOO in modo formale.

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.

9.2 Gestione dei procedimenti amministrativi

I procedimenti amministrativi sono descritti nel "Catalogo dei procedimenti amministrativi", di cui il Responsabile cura l'aggiornamento, estemporaneo o periodico.

I procedimenti amministrativi costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'amministrazione/AOO.

All'interno del catalogo i procedimenti sono individuati mediante la definizione dei riferimenti riportati al successivo paragrafo.

La definizione del singolo procedimento amministrativo rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.

Il risultato concreto di questa attività sono i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare.

9.3 Catalogo dei procedimenti amministrativi

La gestione delle attività e dei procedimenti amministrativi, il loro iter, l'individuazione del responsabile del provvedimento finale e i termini entro i quali il procedimento deve essere concluso sono definiti così come previsto da norme di rango legislativo, regolamentare nonché dal regolamento interno emanato dall'amministrazione.

A tal fine l'AOO, per favorire la trasparenza dell'azione amministrativa, per semplificare i procedimenti e per schematizzare le descrizioni, costituisce una base informativa dei procedimenti amministrativi registrando, per ciascuno di essi, almeno, le informazioni richieste dall'art. 35 del D.Lgs. n. 33/2013 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*".

9.4 Avvio dei procedimenti e gestione degli stati di avanzamento

Mediante l'assegnazione dei fascicoli agli Uffici di volta in volta competenti, si provvede a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente.

La registrazione degli stati di avanzamento dei procedimenti amministrativi sulla base informativa sopra richiamata può avvenire in modalità manuale o automatica.

Nel primo caso, gli stati di avanzamento sono aggiornati dal Responsabile.

Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

10. MODALITA' DI UTILIZZO DEL SISTEMA DI PROTOCOLLO INFORMATICO (art. 5, comma 2, lettera o)

Questa Amministrazione ha adottato come sistema software per la gestione dei flussi documentali la piattaforma applicativa della Società Halley.

Nell'Allegato "*Descrizione Sistema Informatico*" è riportato, nello specifico, la descrizione funzionale ed operativa del suddetto sistema di protocollo informatico, con particolare riferimento alle modalità di utilizzo dello stesso.

11. UFFICIO RESPONSABILE DELLE ATTIVITA' DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI

11.1 Servizio archivistico

L'Ufficio responsabile del Servizio Archivistico (di seguito indicato come servizio archivistico) è funzionalmente e strutturalmente integrato nel suddetto **Ufficio "*Protocollo, Gestione documentale e Archivio*"**. Alla guida del servizio archivistico è posto il Responsabile del servizio per la "*Gestione documentale*" i cui requisiti professionali sono definiti ai sensi dell'art. 61, comma 2 del DPR 28 dicembre 2000, n. 445.

Al servizio archivistico comunale sono attribuiti i seguenti compiti:

- gestire la corretta formazione dell'archivio corrente per mezzo del sistema di gestione informatica dei documenti e conformemente al titolario di classificazione (allegato "Titolario di classificazione" del presente manuale);
- organizzare e garantire le corrette attività di gestione del suddetto archivio, di concerto con le unità organizzative responsabili e i vari responsabili dei procedimenti, in particolare relativamente all'assegnazione dei documenti alle suddette unità organizzative e all'attività di supporto alla costituzione e repertoriazione dei fascicoli, operazioni di competenza dei già citati responsabili dei procedimenti;
- vigilare sulla correttezza delle suddette operazioni svolte dalle singole UOR, ivi comprese le registrazioni di protocollo in uscita, anche ricorrendo a controlli periodici;
- gestire la corretta conservazione degli archivi cartacei dell'ente, prestando particolare attenzione alla corretta gestione degli archivi ibridi, garantendo la salvaguardia del vincolo archivistico anche nel caso che della stessa unità archivistica siano parte documenti sia in formato digitale che in formato analogico.

Il Responsabile del servizio per la "Gestione documentale" inoltre:

- predispone le eventuali modifiche del piano di conservazione dell'archivio e del titolario di classificazione descritti nei rispettivi allegati al presente manuale, qualora siano richieste da sopravvenuti interventi normativi e, comunque, nel rispetto di quanto previsto dall'art. 68, comma 1 del DPR 28 dicembre 2000, n. 445;
- provvede al trasferimento periodico dei fascicoli e delle serie documentarie al sistema di conservazione sotto forma di pacchetti informativi, da lui prodotti, secondo quanto disposto dall'art. 6, comma 3 del DPCM 3/12/2013, "Regole tecniche in materia di sistema di conservazione";
- stabilisce, relativamente ai documenti per cui sono scaduti i tempi previsti dalla conservazione, il trasferimento in conservazione permanente o lo scarto, nel rispetto di quanto previsto dalla normativa vigente, in particolare ai sensi dell'art. 21 del D. Lgs. 22 gennaio 2004, n. 42, dandone comunicazione al responsabile della conservazione che, nel caso di scarto, procede all'eliminazione del pacchetto di archiviazione corrispondente, secondo quanto disposto dall'art. 9, comma 1, lettera l del DPCM 3/12/2013, "Regole tecniche in materia di sistema di conservazione";
- stabilisce i livelli di accesso ai documenti archivistici conservati nonché le forme e le modalità di consultazione interna ed esterna dell'archivio, nel rispetto della normativa vigente in materia di esibizione dei documenti e di tutela della riservatezza dei dati personali, anche nel caso che il sistema di conservazione sia esterno all'ente.

11.2 Servizio della conservazione elettronica dei documenti

In attuazione delle disposizioni contenute nell'art. 44 del D. Lgs. 82/05 (CAD Codice dell'Amministrazione Digitale), il sistema di conservazione è volto ad assicurare, dalla presa in carico dal produttore, la conservazione degli oggetti digitali, garantendo il mantenimento delle loro caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Responsabile della Conservazione, figura centrale del sistema di conservazione, opera d'intesa con il Responsabile del Trattamento dei Dati Personali, con il Responsabile della Sicurezza, con il Responsabile dei Sistemi Informativi e con il Responsabile della Gestione Documentale.

Al Responsabile della Conservazione sono demandati, ai sensi dell'art. 7 DPCM 3/12/2013 (Regole tecniche in materia di conservazione), i seguenti compiti:

a) definizione delle caratteristiche e dei requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, in modo conforme alla normativa vigente;
b) gestione del processo di conservazione, in modo tale da garantirne nel tempo la conformità alla normativa vigente;
c) generazione del rapporto di versamento, conformemente alle modalità previste dal manuale di conservazione;
d) generazione e sottoscrizione del pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) monitoraggio della corretta funzionalità del sistema di conservazione;
f) verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) adozione delle misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adozione di analoghe misure in riferimento all'obsolescenza dei formati;
h) duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art.12 DPCM 3/12/2013 (Regole tecniche in materia di conservazione);
j) assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
m) predisporre il manuale di conservazione di cui all'art. 8 DPCM 3/12/2013 (Regole tecniche in materia di conservazione) e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il ruolo del Responsabile della Conservazione è svolto da un dirigente o da un funzionario formalmente designato; può essere altresì svolto dal Responsabile del Servizio per la tenuta del protocollo, per la gestione dei flussi documentali e degli archivi, ove nominato.

12. SISTEMA DI CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI (art. 5, comma 2, lettera m)

12.1 Protezione e conservazione degli archivi

L'archivio comunale è protetto e conservato ai sensi del decreto legislativo del 22 gennaio 2004, n° 42, il quale prevede, all'art. 10, c. 2, lettera b, il riconoscimento come beni culturali degli archivi e dei singoli documenti dello Stato, delle regioni, degli enti pubblici territoriali e di ogni altro ente ed istituto pubblico.

Il suddetto archivio e i documenti, analogici o informatici, in esso contenuti sono inalienabili (art. 53, c. 2 del già citato decreto) e vengono conservati sin dal momento dell'inserimento di ciascun documento nell'archivio medesimo mediante l'attribuzione di un numero di protocollo e di un codice di classificazione stabilito in base al titolario di cui all'allegato "Titolario di classificazione" del presente manuale o, per i documenti sottoposti a registrazione particolare, dal momento in cui sono registrati secondo quanto specificato nel precedente par.7.10.

L'archivio e l'insieme dei documenti in esso contenuti non possono essere smembrati, distrutti, danneggiati o utilizzati in modo tale da recare pregiudizio alla loro conservazione, come sancito dall'art. 20, c. 1 e 2 del suddetto decreto, ed anzi, ai sensi del successivo art. 30 c. 4, l'archivio viene conservato nella propria organicità, ordinato ed inventariato andando, così, a costituire l'archivio storico.

Gli interventi di spostamento e di trasferimento dal luogo di conservazione dell'archivio di deposito e dell'archivio storico, nonché ogni altro intervento tra quelli previsti dall'art. 21, commi 1 e 2 del suddetto decreto sono sottoposti alla preventiva autorizzazione della soprintendenza archivistica competente per territorio, ivi comprese le operazioni di scarto

dei documenti le quali, se hanno ad oggetto documenti digitali, vengono svolte seguendo le modalità specificate nel par. 13.2 del presente manuale e seguendo le indicazioni contenute nel piano di conservazione allegato al presente manuale, anche in considerazione del fatto che la competenza per la tutela degli archivi pubblici da parte del Ministero dei beni e delle attività culturali e del turismo si esercita anche sui sistemi di conservazione digitale, come ribadito dall'art. 6, c. 9 del DPCM 3/12/2013 contenente le regole tecniche in materia di sistemi di conservazione digitale.

Ai documenti, sia analogici che digitali, contenenti dati personali o riservati si applicano le vigenti disposizioni di legge sulla tutela di detti dati, procedendo a definire gli appropriati livelli di accesso come previsto nel piano di sicurezza e nel paragrafo 13.4 del presente documento.

Questa Amministrazione è consapevole che la protezione e la conservazione degli archivi, in maniera particolare di quelli digitali e di quelli ibridi, si adempiono a partire da una corretta formazione e gestione dell'archivio stesso, pertanto pone particolare attenzione allo svolgimento delle opportune procedure di classificazione e fascicolazione descritte nei successivi paragrafi del presente manuale di gestione che permettono la sedimentazione e l'organizzazione dell'archivio in maniera corretta e ordinata, in modo da rendere più semplice il recupero dei documenti anche a distanza di tempo dalla loro archiviazione.

La sicurezza di tali archivi è, comunque, indissolubilmente connessa anche al rispetto di quanto esplicitato nel manuale di conservazione nonché alla corretta applicazione, sia dal punto di vista procedurale che da quello tecnologico, delle misure di sicurezza previste per il sistema di gestione informatica dei documenti e per il sistema di conservazione dei documenti informatici descritte, rispettivamente, nel piano per la sicurezza dei documenti informatici (capitolo 4 del presente manuale) e nel piano di sicurezza del sistema di conservazione previsto ai sensi dell'art. 12, c. 1 del suddetto DPCM.

12.2 Titolario di classificazione

Questo Ente intende assicurare una corretta organizzazione dei documenti d'archivio prodotti, sulla base di criteri uniformi, in attuazione degli artt. 50, c. 4 e 52, c. 1, lett. f del DPR 28 dicembre 2000, n° 445; a tal fine adotta il titolario di classificazione (o piano di classificazione).

Il titolario di classificazione, un sistema precostituito di partizioni astratte, ordinate gerarchicamente, definito sulla base dell'organizzazione funzionale dell'AOO, è lo strumento utilizzato da questo Ente per organizzare in maniera razionale e ordinata la sedimentazione dei documenti del proprio archivio, in maniera da garantire l'omogenea e coerente collocazione di detti documenti in relazione agli affari o ai procedimenti amministrativi di cui sono parte integrante.

Il titolario adottato dall'Ente è riportato nell'allegato *"Titolario di Classificazione"* del presente manuale. L'articolazione interna del detto schema è strutturata su più livelli di cui quello più elevato individua funzioni primarie e di organizzazione dell'Ente mentre i livelli sottostanti corrispondono a specifiche competenze che rientrano all'interno della funzione primaria descritta dal titolo medesimo.

Il suddetto titolario viene adottato unitamente al presente manuale di gestione di cui è parte integrante e deve avere forma stabile, salvo nel caso in cui si debba procedere ad un suo aggiornamento o revisione, dovuti a modifiche legislative che interessino le

funzioni e le competenze dell'Ente; tali modifiche sono predisposte dal Responsabile del servizio per la "*Gestione documentale*" come specificato nel precedente par. 11.1, approvate con le modalità stabilite nel par. 15.1 del presente documento e, di norma, introdotte a partire dal 1° gennaio dell'anno successivo.

L'operazione che viene eseguita a partire dal titolario è la classificazione ed è finalizzata ad organizzare logicamente, in relazione alle funzioni dell'Ente, tutti i documenti protocollati, siano essi cartacei o informatici.

Tale operazione consiste nell'assegnazione a ciascun documento di un indice di classificazione che, in base all'oggetto del documento medesimo, lo associa alla partizione del titolario relativa alla corrispondente funzione dell'Ente, risultando in tal modo indicata la posizione logica del documento all'interno dell'archivio e permettendone l'inserimento nel fascicolo appropriato.

Nel caso di documenti in entrata, la classificazione è demandata al "Servizio per la Gestione documentale" il quale, eseguita la registrazione di protocollo, associa a ciascun documento la classifica di riferimento prima di trasmetterlo alla UOR cui compete sia la trattazione che la gestione del fascicolo attinente, secondo quanto previsto al successivo paragrafo 12.3.

Se l'indice di classificazione associato al documento non è corretto, la unità organizzativa responsabile assegnataria può provvedere direttamente alla rettifica oppure può rimandare indietro il documento in modo che sia il servizio di protocollo ad apportare le dovute correzioni e procedere ad una nuova assegnazione all'unità di pertinenza. In ogni caso il sistema documentale conserva traccia dei suddetti passaggi. Nel caso, invece, di documenti in uscita o trasmessi internamente ad altre unità organizzative della stessa AOO, la classificazione è di competenza dell'unità organizzativa responsabile che li ha prodotti.

Tutti i soggetti abilitati all'operazione di classificazione dei documenti, nell'ambito dell'AOO, devono conoscere e saper correttamente utilizzare il titolario di classificazione; è compito del responsabile del servizio per la gestione documentale (o del responsabile del servizio archivistico laddove il ruolo non sia ricoperto dalla stessa persona) provvedere affinché detto personale sia adeguatamente formato sul corretto utilizzo dello strumento e debitamente istruito sulle variazioni eventualmente apportate.

L'applicazione del detto titolario e delle sue eventuali modifiche, non è mai retroattiva, anche in considerazione del fatto che deve essere mantenuto nel tempo il legame dei fascicoli e dei documenti dell'archivio con la struttura del titolario vigente al momento della produzione degli stessi e, dunque, il corretto vincolo archivistico che lega la produzione documentaria dell'ente all'attività e alle funzioni dello stesso; proprio a tal fine viene garantita la storicizzazione delle variazioni del titolario e la possibilità di ricostruire le diverse voci nel tempo. Il sistema di gestione informatica dei documenti consente nel caso il titolario sia stato modificato secondo le modalità espresse in precedenza, la possibilità di inserire nuovi documenti nei fascicoli già aperti, fino alla chiusura degli stessi.

12.3 Formazione e identificazione dei fascicoli

Fascicolazione dei documenti

I documenti entrati a far parte del sistema informatico, indipendentemente dal supporto sul quale sono prodotti, sono riuniti in fascicoli, mediante l'operazione di fascicolazione che

consiste nell'inserire ciascun documento nel fascicolo di riferimento, all'interno della corrispondente partizione logica prevista dal titolario di classificazione dell'Ente.

Tale operazione risulta fondamentale per la gestione e l'uso dell'archivio in quanto consente di collegare i singoli documenti a quelli precedenti e successivi prodotti nell'ambito di uno stesso procedimento amministrativo, affare o attività, in modo da riflettere il concreto espletamento delle funzioni dell'Ente; il collegamento sarà, ovviamente, di tipo logico se i documenti sono informatici e di tipo fisico se, invece, sono cartacei.

Il fascicolo costituisce l'unità di base dell'archivio ed è indivisibile, i documenti sono collocati al suo interno secondo l'ordine cronologico di registrazione sul sistema di gestione informatica dei documenti.

Ogni fascicolo all'interno dell'archivio dell'Ente va ad occupare un posto specifico, definito in base al titolario di classificazione di cui all'allegato *"Titolario di Classificazione"* del presente manuale, tale posizione è di natura logica, nel caso di fascicoli informatici, o fisica, nel caso di fascicoli cartacei o di parti cartacee dei fascicoli ibridi.

Tipologie di fascicoli

Genericamente, all'interno di un archivio, possono distinguersi tre tipologie di fascicoli:

- **fascicoli per affare o per procedimento amministrativo**: si aprono nel livello più basso tra quelli previsti dal titolario di classificazione. Contengono documenti relativi alla trattazione di uno stesso procedimento amministrativo e recanti la medesima classifica. Tali fascicoli restano aperti per tutto il tempo di trattazione dell'affare medesimo.
- **fascicoli relativi a persone fisiche o giuridiche**: possono essere aperti in qualsiasi livello del titolario, non necessariamente al livello più basso e contengono documenti di classifiche diverse (ad esempio, nei comuni, i fascicoli del personale vengono aperti a livello di titolo III e ciascuno di essi contiene tutta la documentazione relativa al rapporto tra l'ente e il dipendente cui il fascicolo si riferisce, anche se i vari documenti necessariamente fanno riferimento a diverse classi). Tali fascicoli, generalmente, restano aperti per periodi di tempo anche molto lunghi e si procede alla chiusura soltanto quando cessa il rapporto tra detta persona fisica o giuridica e l'ente,
- **fascicoli per attività**: comprendono i documenti prodotti nello svolgimento di un'attività amministrativa semplice che in genere comporta meri adempimenti. I documenti all'interno recano tutti la stessa classifica, con oggetti uguali o simili e destinatari diversi; la durata di detti fascicoli è annuale.

Apertura del fascicolo

La responsabilità della corretta formazione e gestione dei fascicoli per procedimento o per affare è di competenza dei Responsabili dei procedimenti amministrativi, individuati all'interno delle singole unità organizzative responsabili incaricate della trattazione degli affari medesimi.

Documenti in ingresso

L'Ufficio "*Protocollo, Gestione documentale e Archivio*", dopo aver proceduto alla registrazione di protocollo e alla classificazione, trasmette il documento all'unità organizzativa cui compete il trattamento. Il Responsabile del procedimento individuato all'interno dell'unità organizzativa medesima provvede, a seconda dei casi, ad inserire il

documento in un fascicolo già esistente o, qualora la situazione lo richieda, ad aprire un nuovo fascicolo.

Documenti in uscita

Nel caso, invece, di documenti in uscita o trasmessi ad altra unità organizzativa di riferimento all'interno dell'AOO, spetta alle unità organizzative che abbiano prodotto i documenti medesimi eseguire la registrazione di protocollo, la classificazione e la fascicolazione, prima di procedere alla trasmissione degli stessi.

Identificazione del fascicolo

Nel sistema di gestione informatica dei documenti a ciascun fascicolo vanno associate almeno le seguenti informazioni, che lo identificano all'interno dell'archivio:

- l'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo,
- le eventuali altre amministrazioni partecipanti,
- il responsabile del procedimento,
- la data di apertura,
- l'indice di classificazione,
- il numero del fascicolo (un identificativo univoco, cronologicamente progressivo, attribuito automaticamente dal sistema al momento dell'apertura di ogni nuovo fascicolo),
- l'oggetto del procedimento,
- l'elenco dei documenti contenuti.

Le informazioni suindicate, anche dette *metadati*, vanno riportate anche sulla "camicia" cartacea del fascicolo.

L'inserimento delle informazioni precedentemente elencate consente al sistema informatico di formare il repertorio dei fascicoli, un elenco progressivo degli stessi in ordine cronologico di apertura che permette il reperimento di ciascun fascicolo con tutti i metadati associati.

Al fine di agevolare la gestione successiva, possono essere associate al fascicolo ulteriori informazioni, come ad esempio i tempi previsti per lo scarto o l'eventuale trasferimento in conservazione permanente.

L'inserimento di tutti i suddetti metadati nel sistema di gestione informatica dei documenti è di competenza del responsabile del procedimento della unità organizzativa responsabile cui è demandata la trattazione dell'affare.

Assegnazione del fascicolo

All'interno delle singole unità organizzative responsabili, i dirigenti hanno il compito di eseguire l'assegnazione delle pratiche da trattare ai singoli responsabili dei procedimenti designati, definendo, per mezzo del sistema di gestione informatica dei documenti, specifici livelli di accesso e riservatezza a ciascun fascicolo.

Chiusura del fascicolo

Al termine di ciascun procedimento amministrativo, il responsabile del procedimento procede alla chiusura del relativo fascicolo, associandogli la data di chiusura che fa riferimento alla registrazione nel sistema dell'ultimo documento prodotto nel corso della trattazione dell'affare. Il sistema di gestione informatica dei documenti, in relazione alle date apposte, evidenzia in maniera chiara per ciascun fascicolo consultato se è aperto o chiuso.

Sottofascicoli e serie di fascicoli

I fascicoli, qualora se ne avverta l'esigenza ai fini operativi o in considerazione dell'eccessiva mole di documenti contenuti, possono essere al loro interno articolati in sottofascicoli e questi, a loro volta, in inserti, salvaguardando però sempre il principio archivistico che il fascicolo resta un'unica entità indivisibile, pertanto, tali partizioni interne sono visualizzate sul sistema di gestione informatica dei documenti risultando accessibili dal fascicolo di riferimento e sono identificate, all'interno di questo, con un proprio numero e oggetto.

Il sistema di gestione documentale consente inoltre di collegare tra loro più fascicoli, nel caso esigenze operative imponessero di creare aggregazioni per gestire procedimenti amministrativi particolarmente complessi e articolati o si reputasse necessario formare delle serie; in tal caso è possibile disporre di un immediato collegamento che salvaguardi il vincolo archivistico che lega detti fascicoli tra loro e permetta, all'occorrenza, l'immediato reperimento del fascicolo che interessa. Nel caso di fascicoli cartacei o di documenti cartacei parte di fascicoli ibridi, è necessario che la "camicia" dell'incartamento rechi le informazioni relative ai sottofascicoli e agli inserti contenuti, nonché alle eventuali serie o aggregazioni di cui il fascicolo è parte.

I fascicoli e le serie documentarie relative a procedimenti e affari conclusi sono trasferiti nell'archivio di deposito dell'ente, secondo quanto disposto dall'art. 67 del DPR 28 dicembre 2000, n. 445. Per la documentazione informatica, fatto salvo quanto espresso dalla suddetta norma, l'obbligo si assolve trasferendo il pacchetto informativo di versamento, contenente le unità archivistiche e i relativi metadati, al sistema di conservazione, secondo quanto previsto ai sensi dell'art. 6, c. 3 del DPCM 3/12/2013 "regole tecniche in materia di sistema di conservazione" e conformemente alle modalità descritte nel manuale di conservazione.

13. ARCHIVIAZIONE E CONSERVAZIONE DEI DOCUMENTI (art. 5, comma 2, lettere m e p)

13.1 L'archivio dell'amministrazione

L'archivio consiste nella raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle proprie funzioni, per il conseguimento dei propri fini istituzionali. L'archivio informatico è costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.

Gli atti formati o ricevuti dall'Amministrazione o dalla Area Organizzativa Omogenea (AOO) sono legati tra loro dal vincolo archivistico: nesso che collega in maniera logica la documentazione posta in essere dal soggetto produttore. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio in senso proprio costituisce un complesso unitario, tuttavia, per motivi organizzativi e funzionali, esso viene suddiviso in tre sezioni: archivio corrente, archivio di deposito e archivio storico.

Archivio corrente (Documenti attivi)

L'archivio corrente è costituito dal complesso organico dei documenti prodotti, acquisiti e conservati dalla AOO nell'esercizio delle proprie funzioni, relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione e per i quali sussista un interesse attuale.

Possiamo, pertanto, affermare che è costituito da tutti i documenti appartenenti a fascicoli aperti ed agli affari correnti. La gestione dell'archivio viene eseguita nel rispetto del piano di classificazione adottato.

L'archivio corrente è collegato al sistema di protocollo. Secondo tale requisito tutto l'archivio corrente è gestito attraverso un sistema informatico che ne garantisce la corretta memorizzazione, e archiviazione assicurandone nel tempo l'accessibilità e la consultabilità.

Archivio di deposito (Documenti semi-attivi)

L'archivio di deposito è costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per lo svolgimento delle attività amministrative correnti, ma che possono rivelarsi ancora utili per finalità amministrative e giuridiche.

Esso è, quindi, costituito dai documenti relativi a fascicoli ed affari conclusi. L'archivio di deposito consente solo operazioni di consultazione e mantiene i documenti per il numero di anni previsti dalla normativa vigente (fino a 40 anni).

Il sistema informatico fornisce gli strumenti per la selezione dall'archivio corrente dei fascicoli chiusi ed il relativo travaso nell'archivio di deposito. Tali funzioni si appoggiano alle informazioni mantenute nel piano di classificazione adottato.

Tutto l'archivio di deposito è gestito attraverso sistemi informatici che ne garantiscano la corretta memorizzazione, e archiviazione assicurandone nel tempo l'accessibilità e la consultabilità.

Archivio storico (documenti inattivi)

Costituito dal complesso dei documenti prodotti o acquisiti dal soggetto produttore relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle procedure di selezione e scarto, alla conservazione permanente.

13.2 Procedure di selezione e scarto

Le attività di selezione e scarto della documentazione archivistica sono funzionali ai fini della corretta formazione e conservazione della memoria storica dell'Ente, nonché alla migliore consultabilità dell'archivio. I documenti destinati allo scarto sono genericamente intesi come quelli che hanno perso la loro valenza amministrativa, senza assumere alcuna rilevanza storica, ragione per cui, nell'impossibilità pratica di conservare indiscriminatamente ogni documento, occorre effettuare la selezione.

Le operazioni in oggetto, per quanto attiene alla documentazione cartacea, avvengono nell'archivio di deposito dell'Ente, dove si procede al vaglio del materiale allo scopo di definire quale debba essere scartato e quale, viceversa, sia da destinare alla conservazione permanente nell'archivio storico.

Per quanto attiene alla documentazione informatica, conservata presso una struttura di conservazione, il trasferimento in conservazione permanente sarà di tipo logico, distinguendo per mezzo di opportuni metadati, previsti nel manuale di conservazione, il materiale per cui non sia trascorso ancora il tempo stabilito per lo scarto da quello destinato ad essere conservato indefinitamente.

Lo strumento utilizzato per le operazioni di selezione e scarto è il piano di conservazione dell'archivio dell'Ente, Allegato "Piano di Conservazione" del presente manuale, nel quale

sono dettagliate per ciascuna tipologia documentaria, le indicazioni relative ai tempi di conservazione.

Le procedure di selezione e scarto sono svolte annualmente e in ogni caso prima del trasferimento dei documenti all'archivio storico.

Il Responsabile del servizio per la "*Gestione documentale*", relativamente alla selezione della documentazione cartacea, predispone un elenco delle unità archivistiche che si intende scartare, su proposta dei responsabili del procedimento delle varie unità organizzative responsabili che hanno curato la formazione e la gestione dei fascicoli, coadiuvato dal responsabile del servizio archivistico, qualora questa mansione sia ricoperta da altra persona.

Trattandosi di intervento soggetto ad autorizzazione ai sensi dell'art. 21 del D. Lgs. 22 gennaio 2004, n. 42, l'elenco di scarto viene sottoposto alla soprintendenza archivistica competente per territorio, a cui si richiede formalmente l'autorizzazione per poter procedere. Soltanto una volta che il nulla osta sia stato ottenuto si può avviare l'eliminazione fisica dei documenti, che deve avvenire nel rispetto della normativa vigente, in particolar modo per quanto riguarda la tutela dei dati sensibili e personali. Completate le operazioni, il responsabile del servizio per la gestione documentale comunica formalmente alla detta soprintendenza che lo scarto è avvenuto.

I documenti, i cui affari siano esauriti da almeno quaranta anni, destinati alla conservazione permanente sono trasferiti nell'archivio storico conformemente a quanto previsto dall'art. 69 del DPR 28 dicembre 2000, n. 445. L'archivio storico deve essere ordinato e inventariato e l'inventario, aggiornato a seguito del versamento del suddetto materiale, deve essere trasmesso alla soprintendenza archivistica.

Per quanto riguarda la documentazione informatica affidata ad un soggetto conservatore esterno all'Ente, le responsabilità connesse alle procedure di scarto restano in capo al responsabile del servizio per la gestione documentale, il quale riceve comunicazione dal responsabile della conservazione relativamente alla documentazione per cui siano decorsi i tempi previsti per lo scarto.

Il responsabile del servizio per la gestione documentale procede, analogamente a quanto descritto per la documentazione cartacea, a richiedere l'autorizzazione alla competente soprintendenza, presentando anche in questo caso l'elenco del materiale da scartare e, in caso di assenso, autorizza il responsabile della conservazione, per mezzo di un atto formale dell'Ente a procedere all'eliminazione dal sistema dei pacchetti di archiviazione corrispondenti. Eseguita la procedura, il responsabile della conservazione ne fornisce adeguata documentazione all'Ente che, per il tramite del responsabile del servizio di gestione documentale, informa la soprintendenza dell'avvenuto scarto, in considerazione del fatto che resta ferma la competenza del Ministero dei beni e delle attività culturali e del turismo in materia di tutela degli archivi, come espressamente previsto dall'art. 6, c. 9 del DPCM 3/12/2013 "regole tecniche in materia di conservazione".

13.3 Piano di conservazione dell'archivio

In attuazione dell'art. 68 del DPR 28 dicembre 2000 n. 445 questa Amministrazione, attraverso il servizio per la gestione documentale, si dota di un piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti, nel rispetto delle disposizioni in materia di tutela dei beni culturali.

Appare importante sottolineare come dal dettato normativo si evinca che il piano di conservazione sia strettamente connesso al Titolario di classificazione.

Viene tenuta traccia dei documenti che vengono prelevati dagli archivi, registrando ogni movimento effettuato e le richieste di prelevamento. A tal avviso, per l'archiviazione e la custodia dei documenti che contengano dati personali, si applicano le disposizioni normative sulla tutela della riservatezza dei dati personali.

13.4 Criteri e modalità di accesso interno ed esterno alle informazioni documentali

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione/AOO oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

13.4.1 Consultazione ai fini giuridico amministrativi

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15 che qui di seguito si Riporta: "Esclusione dal diritto di accesso.

1. Il diritto di accesso è escluso:
   a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
   b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
   c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
   d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
   a) quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità

nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;

b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
e) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici.

Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale".

13.4.2 Consultazione per scopi storici

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata dal regolamento emanato da ciascuna amministrazione/AOO. Per le amministrazioni/AOO non statali il regolamento è emanato sulla base degli indirizzi generali stabiliti dal Ministero per i beni e le attività culturali (a norma dell'art. 124 del decreto legislativo 22 gennaio 2004, n. 42).

La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'interno (a norma dell'art. 125 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione/AOO. È possibile l'ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);
- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

13.4.3 Consultazione da parte di personale esterno all'Amministrazione

La domanda di accesso ai documenti viene presentata all'Ufficio "Protocollo, Gestione documentale e Archivio" o all'Ufficio "*Relazioni con il Pubblico*" (URP), che provvede a smistarla al servizio archivistico.

Sul sito web dell'Amministrazione è disponibile on line un modulo da compilare per presentare domanda di accesso come quello riportato nell'Allegato " Moduli e schemi".

Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla soprintendenza per i beni archivistici territorialmente competente, con apposito modulo da questa predisposto.

Le domande vengono evase durante gli orari di apertura al pubblico dell'URP e dell'archivio con la massima tempestività.

Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.

In tale caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.

L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico.

La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.

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

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.

13.4.4 Consultazione da parte di personale interno all'Amministrazione

Gli uffici dell'Ente, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica.

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

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, l'unità organizzativa di riferimento e la firma del richiedente stesso.

Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile per la "Gestione documentale" in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali

note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.

Il Responsabile per la "Gestione documentale" verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo.

Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'amministrazione/AOO.

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

14. DEFINIZIONI E ACRONIMI

Termine/Acronimo	Descrizione
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 (AgID), 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.
AgID	**Agenzia per l'Italia Digitale**: organismo che svolge attività di progettazione e coordinamento delle iniziative strategiche per la più efficace erogazione di servizi in rete della pubblica amministrazione a cittadini e imprese. Elabora gli indirizzi, le regole tecniche e le linee guida per la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione Europea, assicura l'uniformità tecnica dei sistemi informativi pubblici destinati a erogare servizi ai cittadini e alle imprese, garantendo livelli omogenei di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo.
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.
AOO	**Area Organizzativa Omogenea**: Insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'art. 50, comma 4 del D.P.R. 28 dicembre 2000, n. 445.
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura, formati, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento della propria attività.
Archivio corrente	Parte di documentazione relativa a pratiche e a procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse corrente.

Termine/Acronimo	Descrizione
Archivio di deposito	Parte di documentazione relativa a pratiche e a procedimenti conclusi, non più occorrenti quindi alla trattazione di pratiche in corso, ma non ancora destinata istituzionalmente alla conservazione permanente.
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
Archivio storico	Complesso di documenti relativi a procedimenti conclusi da più di 40 anni e destinati, previe operazioni di scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico.
Assegnazione	Operazione d'individuazione dell'ufficio utente competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono.
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.
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.
Classificazione	Operazione che consente di organizzare logicamente i documenti in relazione alle funzioni ed alle modalità operative dell'Amministrazione, in base al titolario di classificazione.
Codice o CAD	**Codice dell'Amministrazione Digitale**: Decreto Legislativo del 7 marzo 2005, n. 82, "Codice dell'Amministrazione digitale" (G.U. n. 112 del 16-05-2005 – Suppl. Ordinario n. 93)
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione, al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione.
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
Copia di rispetto	Copia di backup degli archivi
Documento amministrativo	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.
Documento informatico	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Fascicolazione	Operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi

Termine/Acronimo	Descrizione
Fascicolo	Unità archivistica indivisibile di base che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare.
Firma digitale	Risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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. All'articolo 21, il D.Lgs. 82/2005 stabilisce, con un rimando all'art. 2702 del Codice Civile, che la firma digitale (o altra firma elettronica qualificata) fa piena prova fino a querela di falso se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta, equiparando così il documento informatico sottoscritto con firma digitale alla scrittura privata sottoscritta con firma autografa (e non, come avveniva in precedenza, alla scrittura privata con firma autenticata).
Firma elettronica	Insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica": è quindi la forma più debole di firma in ambito informatico, in quanto non prevede meccanismi di autenticazione del firmatario o di integrità del dato firmato.
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma elettronica qualificata	La firma elettronica qualificata è definita come la firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità è certificata da un certificato qualificato. È inoltre richiesto l'uso del dispositivo di firma sicuro, capace cioè di proteggere efficacemente la segretezza della chiave privata. Inoltre, la firma stessa deve essere in grado di rilevare qualsiasi alterazione del documento avvenuta dopo l'apposizione della firma stessa. Qualunque tecnologia che permetta tale identificazione univoca, rientra nel concetto di "firma elettronica qualificata".
Firma grafometrica	E' una modalità di firma che possiede requisiti informatici e giuridici che consentono per legge di qualificarla come "firma elettronica avanzata". I documenti che il dichiarante sottoscrive con la firma grafometrica sono documenti informatici che, sul piano giuridico, hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa e che, sul piano tecnico, soddisfano i requisiti di sicurezza definiti dalla normativa vigente.
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;

Termine/Acronimo	Descrizione
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza 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.
Gestione dei documenti	Insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione, archiviazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione adottato.
HSM	Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.
Impronta di un documento informatico	Sequenza di simboli binari (bit) di lunghezza predefinita, generata mediante l'applicazione di una opportuna funzione di hash, in grado di identificarne univocamente il contenuto.
Marca temporale	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;
Piano di conservazione degli archivi	Piano, integrato con il sistema di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali.
Responsabile della Gestione documentale	Altrimenti detto **Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi**: dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 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.
Segnatura di protocollo	Apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti.
Supporto di memorizzazione	Mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso.
Testo Unico	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, pubblicato con DPR 28 dicembre 2000, n. 445 e successive modifiche ed integrazioni.
Titolario di classificazione	Sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta.

Termine/Acronimo	Descrizione
Ufficio utente	Ufficio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti.
UO	**Ufficio Operativo**: ufficio dell'AOO che svolge le attività afferenti ad un determinato servizio dell'Ente.
UOR	**Unità Organizzativa di Riferimento**: insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

15. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

15.1 Modalità di approvazione e aggiornamento del manuale

Il presente "Manuale di gestione" è adottato con deliberazione di Giunta Comunale su proposta del Responsabile della gestione documentale.

Lo stesso è soggetto a revisione ordinaria ogni anno, su iniziativa del Responsabile della gestione documentale.

Nell'aggiornamento del Manuale si terrà conto di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- variazioni organizzative;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal Responsabile per la "*Gestione documentale*".

La modifica o l'aggiornamento di uno o di tutti gli allegati al presente Manuale non comporta la revisione nei modi di cui sopra del Manuale stesso.

15.2 Regolamenti abrogati

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

15.3 Pubblicità del presente manuale

Il Responsabile per la "*Gestione documentale*" propone lo schema di manuale e, successivamente, ne cura la tenuta e l'aggiornamento nel tempo, quindi si fa carico della corretta applicazione e conservazione dello stesso, nonché della sua distribuzione e pubblicazione.

15.4 Operatività del presente manuale

Il presente regolamento è operativo il primo giorno del mese successivo a quello della sua adozione.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Piano di Sicurezza

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato viene riportato il Piano di sicurezza dei documenti informatici adottato dall'Ente.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 Premessa

Nel rispetto dell'approccio metodologico descritto nel capitolo 4 del Manuale di Gestione documentale il presente piano di sicurezza è strutturato nei seguenti argomenti:

- organizzazione dell'Ente ed organigramma di tutti i soggetti che provvedono al trattamento dei dati personali, con una descrizione dei ruoli, delle mansioni e delle responsabilità;
- censimento dei trattamenti di documenti con procedure informatiche e misure di sicurezza adottate;
- rilevazione dei luoghi fisici e delle misure di sicurezza già adottate dall'Ente;
- rilevazione del livello di informatizzazione dell'Ente e delle misure di sicurezza eventualmente adottate dall'Ente, svolto attraverso un accurato censimento delle risorse hw e sw utilizzate per la gestione documentale
- analisi dei rischi;
- valutazione delle possibili soluzioni adottabili per il raggiungimento dei livelli di sicurezza richiesti dal D.Lgs 196/03 e dal relativo allegato B (disciplinare tecnico).

2 Distribuzione di compiti e responsabilità

Nella procedura organizzativa "*Aree Organizzative Omogenee ed Organizzazione*" è riportato l'organigramma di tutti i soggetti che nell'ambito dell'Ente provvedono al trattamento dei documenti, con una descrizione di ruoli, mansioni e responsabilità.

In essa è anche specificato l'affidatario del ruolo di Amministratore del Sistema informativo comunale di Arpaise, in attuazione del punto c) del provvedimento del Garante del 27-11-2008 pubblicato in gazzetta ufficiale n. 300 del 24-12-2008 "Funzioni di amministrazione di sistema".

Nella procedura organizzativa "*Amministratori di Sistema*" si riportano informazioni sulle modalità con cui questo Ente amministra il Sistema Informativo e le funzioni affidate all'Amministratore stesso.

3 Censimento dei trattamenti dei documenti e aspetti di sicurezza correlati

La gestione di documenti digitali effettuati dall'Ente si articola nelle operazioni ampiamente descritte in questo Manuale che quì si elencano:

- Formazione
- Registrazione, classificazione e fascicolazione
- Archiviazione nel repository documentale
- Accesso ai documenti informatici e consultazione
- Trasmissione e interscambio
- Conservazione dei documenti informatici
  - *Servizio archivistico*
  - *Servizio di conservazione a norma*
  - *Conservazione dei documenti informatici e delle registrazioni di protocollo*
  - *Conservazione delle registrazioni di sicurezza*

In questo paragrafo vengono riesaminati, uno per volta, tutti i trattamenti sopra censiti evidenziando gli aspetti di sicurezza che li riguardano.

3.1 Formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e tra AOO diverse.

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

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale fa sì che non si possa definire in modo statico l'elenco di formati validi per la formazione dei documenti, pertanto occorre fare riferimento all'elenco dei formati pubblicati online sul sito dell'Agenzia per l'Italia digitale che viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati.

Nell'allegato "Formati dei documenti elettronici", è riportato l'elenco dei formati attualmente accettati da questo Ente.

I documenti informatici prodotti dall'AOO con prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

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 di cui al decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (regole tecniche in materia di generazione e verifica delle firme elettroniche avanzate, qualificate e digitali …"). L'allegato "Sottoscrizione dei documenti informatici" descrive le regole per l'uso della firma elettronica e digitale all'interno dell'Ente e fornisce l'elenco dei documenti prodotti dall'Ente, soggetti o meno alla sottoscrizione con firma digitale.

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.

3.2 Gestione dei documenti informatici

L'art. 7 del D.P.C.M. 03/12/2013 ha ripreso, aggiornandoli, i requisiti minimi di sicurezza che devono soddisfare i sistemi di protocollo informatico. Essi sono i seguenti: "

1. *il **sistema di protocollo informatico** assicura:*
   a. *l'univoca identificazione ed autenticazione degli utenti;*
   b. *la protezione delle informazioni relative a ciascun utente nei confronti degli altri;*
   c. *la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;*
   d. *la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione;*
2. *il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;*
3. *il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore;*
4. *le registrazioni di cui ai commi 1, lettera d), e 3 devono essere protette da modifiche non autorizzate;*
5. *il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto;*
6. *il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196."*

Le **registrazioni di sicurezza** sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul sistema informatico di protocollo - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico [Intrusion Detection System (IDS), sensori di rete e firewall];
- dalle registrazioni del sistema informatico di protocollo.

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 Servizio per la gestione documentale e dal titolare dei dati e, ove previsto, dalle forze dell'ordine.

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

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione, 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.

All'esterno della AOO

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla Circolare n. 60 del 23 gennaio 2013 che definisce il formato e la tipologia di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni, opera una revisione della circolare AIPA/CR/28 del 7 maggio 2001 abrogandola e sostituendola a decorrere dalla conclusione dell'iter di emanazione dei decreti attuativi delle disposizioni del Codice dell'Amministrazione Digitale in materia di documento informatico e gestione documentale, protocollo informatico e di formazione e conservazione dei documenti informatici.

All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

3.4 Accesso ai documenti informatici

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

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Nell'allegato "Abilitazioni all'utilizzo del sistema informatico di protocollo" esse vengono schematizzate.

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password sono riportate nell'Allegato "Politiche di sicurezza".

Il sistema informatico di protocollo adottato dall'Amministrazione/AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del sistema può accedere solamente ai documenti che sono stati assegnati alla propria unità organizzativa o agli uffici ad essa subordinati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal Responsabile del Servizio per la gestione documentale dell'Amministrazione/AOO. Tali livelli si distinguono in:

- abilitazione alla consultazione,
- abilitazione all'inserimento,
- abilitazione alla cancellazione
- abilitazione alla modifica delle informazioni.

Utenti esterni alla AOO – altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le AOO che accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'ufficio di appartenenza del Responsabile del Procedimento.

Utenti esterni alla AOO - privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative:

1. l'accesso diretto per via telematica
2. l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.

L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.

Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.

Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

3.5 Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nel D.P.C.M. 03/12/2013 "Regole tecniche per la conservazione" e nella Circolare dell'Agenzia per l'Italia Digitale n. 65 del 10 aprile 2014.

Servizio archivistico

Il responsabile del sistema archivistico dell'AOO ha individuato la sede dell'archivio dell'amministrazione già attiva per questa funzione.

Il responsabile del servizio in argomento ha effettuato la scelta a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza).

Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.

Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.

Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti.

Servizio di conservazione sostitutiva

Il responsabile della conservazione sostitutiva dei documenti, operando d'intesa con i responsabili del trattamento dei dati personali, della sicurezza e dei sistemi informativi, provvede, tra l'altro alla

a) verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
b) adozione delle misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adozione di analoghe misure in riferimento all'obsolescenza dei formati;
c) duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
d) adozione delle misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art.12 DPCM 3/12/2013 (Regole tecniche in materia di conservazione).

4 Il sistema informatico di supporto alla gestione documentale

Durante l'intervento nella/e sede/i dell'Ente è stato visionato il sistema informativo attraverso le sue componenti hardware e software e sono state rilevate le misure di sicurezza intraprese dall'Ente su tali risorse.

Il RSP ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza trimestrale durante la fase di esercizio;
- 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 entro sette giorni in caso di disastro;
- conservazione, a cura dei servizi informatici 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 Sistema di Protocollo Informatico;
- 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.

5 Analisi dei rischi

5.1 Fattori di rischio per la sicurezza

L'analisi dei rischi è uno dei più importanti elementi per inquadrare i rischi ed individuare le appropriate misure di sicurezza[1].

I rischi che vengono presi in considerazione sono di due tipi, a seconda che riguardino il rispetto delle imposizioni del codice della privacy, oppure il più vasto mondo dei rischi propri di un sistema informativo.

La differenza tra le due categorie di rischi è fondamentale, perché mentre nella seconda categoria sono compresi tutti i rischi della prima, nella prima categoria sono contemplati solo quei rischi, direttamente afferenti alla tutela dei dati personali.

In altri termini, se un sistema informativo che gestisce servizi al pubblico si arresta alle ore 10 del mattino di un giorno feriale, per mancanza di energia al server centrale, i clienti diventano impazienti, gli operatori di sportello tempestano di telefonate il centro elettronico, la direzione viene inondata di proteste, ma le disposizioni del codice sulla protezione dei dati personali non vengono violate, perché siamo ancora ben lontani dai tempi di ripristino del servizio di trattamento, indicati dal codice stesso.

Si vede subito che la differenza fra le misure minime e le misure necessarie non è quindi solo legata allo stato dell'arte delle misure, ma anche alle misure stesse che possono garantire da certi rischi ritenuti molto grandi, ma di cui la legge ignora l'esistenza perché non afferenti alla protezione di dati personali.

L'analisi di rischio sarà quindi volta ad identificare, valutare e contrastare

- i rischi propri indicati dalla legge, e cioè il rischio di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- i rischi individuati nella gestione del sistema informativo.

Alla prima categoria si bada per obbligo di legge; alla seconda categoria occorre badare per garantire il regolare svolgimento dell'attività esercitata e la continuità dei servizi ai cittadini.

Più l'analisi dei rischi viene fatta accuratamente, anche per rischi non legati specificatamente al trattamento di dati personali, più questo allegato rappresenta in modo esauriente e completo il manuale per la sicurezza del sistema informativo, che include tutte le misure atte a tutelare la privacy, ma che comprende anche tutte le misure rilevantissime per la sopravvivenza dell'Ente stesso.

Nell'analisi di impatto che segue si prendono in considerazione le seguenti macro-categorie di rischi, connesse all'utilizzo di sistemi di elaborazione, che possono generare danni e che comportano quindi rischi per la sicurezza dei dati:

- ***Uso non autorizzato dell'Hardware (Unah)***
- ***Rivelazione illegittima di informazioni, anche per negligenza (Riin)***
- ***Alterazione non autorizzata di informazioni (Anai)***
- ***Perdita di informazioni (Prin)***
- ***Uso non autorizzato di informazioni (Unai)***

[1] Il modello di analisi dei rischi proposto in questo capitolo è stato elaborato sulla base di principi utilizzati nel campo del risk management tipici dell'ingegneria del software e applicato, con i dovuti adattamenti, al settore della sicurezza. Il modello è stato, poi, sperimentato in alcune decine di Enti Locali in occasione dell'adeguamento al D.Lgs. 196/2003, per la messa in sicurezza dei sistemi informativi e per la protezione dei dati personali trattati.

- ***Uso non autorizzato di applicativi (Unaa)***
- ***Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie (Psup)***

e si valuta l'impatto sulla sicurezza che ha ognuna delle macro-categorie di rischio suddette.

Quindi, per ognuna delle macrocategorie di rischio individuate, si esamina un ulteriore e più dettagliato ventaglio di **fattori di rischio** che risultano critici per la sicurezza dei dati trattati nell'Ente.

Nella tabella seguente si riportano i fattori di rischio individuati:

Fattori di Rischio	Descrizione dell'impatto sulla sicurezza
Furto di credenziali di autenticazione per l'accesso ad un computer	Permette all'intruso di poter accedere ad una stazione di lavoro o ad un server con le autorizzazioni legate alle credenziali sottratte e arrecare qualsiasi tipo di danno ai dati trattati.
Utilizzo potenza di calcolo a propri fini	In questo contesto si inquadra il trattamento non consentito o non conforme di dati personali (violazione dell'art. 167 - illecito penale).
Azione di virus informatici o di codici malefici	Tali programmi potrebbero alterare il funzionamento delle applicazioni software. L'azione dei programmi non conosciuti o nascosti è tra le forme più insidiose di danneggiamento che possono essere arrecate agli strumenti elettronici.
Spamming o altre tecniche di sabotaggio	Tutte le forme di ingolfamento dei sistemi elettronici e quelle di sabotaggio sono soggette alle azioni previste dal codice civile e penale.
Furto di credenziali di autenticazione per l'accesso alle applicazioni software censite	Permette all'intruso di poter accedere alla specifica applicazione software con le dovute autorizzazioni legate a quelle credenziali sottratte e arrecare qualsiasi tipo di danno sui dati trattati.
Accesso non autorizzato a informazioni e dati presenti nelle applicazioni software censite	Permette ad utenti autenticati del Sistema Informativo di accedere ad informazioni senza la necessaria autorizzazione ovvero di accedere ad informazioni per le quali non è possibile predisporre un profilo di autorizzazione informatica.
Malfunzionamento, indisponibilità o degrado degli strumenti	Per prevenire situazioni di malfunzionamento hw/sw il Comune deve disporre di contratti di assistenza e manutenzione attivi che permettano il controllo e monitoraggio dell'attività dei sistemi; inoltre è necessario adottare opportune misure di sicurezza al fine di garantire il ripristino dei dati e delle applicazioni software in caso di distruzione degli strumenti.
Guasto tecnologico ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Anche in questi casi è necessario adottare opportune misure di sicurezza al fine di prevenire danni (sistemi di allarme, ...) e, in caso di distruzione degli strumenti, garantire il ripristino dei dati e delle applicazioni software.
Carenza di consapevolezza, disattenzione o incuria	Questo atteggiamento può provocare i maggiori danni su ciascun trattamento da parte dell'incaricato.

Fattori di Rischio	Descrizione dell'impatto sulla sicurezza
Errori umani nella gestione della sicurezza	E' sempre possibile commettere errori nell'adoperare gli strumenti elettronici. Quando viene effettuato un trattamento su dati personali l'incaricato dovrà attenersi alle regole di verifica sull'esattezza delle informazioni trattate. E' necessario impartire le dovute istruzioni agli operatori che trattano direttamente o indirettamente con gli strumenti elettronici.
Comportamenti sleali o fraudolenti	Il trattamento illecito dei dati è soggetto alle sanzioni previste dal codice penale. L'incaricato dovrebbe essere consapevole che il trattamento dei dati personali è soggetto alla tutela così come previsto dal codice D.lgs. 196/2003, dal codice civile (art. 2050) e dagli specifici articoli del codice penale.
Accessi esterni non autorizzati	La regolamentazione degli accessi ai locali del Comune è un aspetto delicato che va affrontato attraverso regole e autorizzazioni a tutti i livelli.
Intercettazione di informazioni in rete	E' necessario, per i sistemi collegati alla rete Internet e intranet, dotarsi di dispositivi che permettano il monitoraggio della rete telematica per consentire l'attuazione di opportune misure di sicurezza a favore del buon funzionamento dei sistemi informativi.
Accessi non autorizzati a locali/reparti ad accesso ristretto	I locali adibiti ad ospitare sistemi e strumenti per il trattamento elettronico dei dati personali vanno protetti da tutti i possibili pericoli per intrusioni o accessi non consentiti.
Asportazione e furto di strumenti contenenti dati	I dispositivi di memorizzazione dei dati devono essere collocati in luoghi sicuri e protetti.
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	In qualsiasi momento i sistemi sono esposti a queste forme di rischio. E' necessario adottare opportune misure di sicurezza al fine di prevenire danni agli strumenti elettronici e garantire, in caso di distruzione, il ripristino dei dati e delle applicazioni in essi contenuti.

L'analisi dei rischi, fatta nel paragrafo 5.3, evidenzia, per ciascuno dei fattori di rischio individuati, il livello di criticità, ovvero il livello di difficoltà da parte dell'Ente di garantire il non accadimento dell'evento dannoso.

5.2 Analisi d'impatto

L'obiettivo di sicurezza è ottenuto in particolare mediante il perseguimento di appropriate misure di sicurezza.

In questo paragrafo viene valutato l'impatto delle macro-categorie di rischio individuate rispetto alla sicurezza dell'Ente; la valutazione viene fatta su una scala che prevede quattro valori qualitativi:

0 = impatto basso
1 = impatto medio
2 = impatto alto; aspetto importante
3 = impatto molto alto; aspetto fondamentale

La valutazione è utilizzata nel seguito del documento per orientare le scelte sulle politiche di sicurezza da adottare.

Le tabelle seguenti sintetizzano i profili delle categorie di rischio specificando, per ogni macrocategoria, l'impatto che quest'ultima ha sulla sicurezza dell'Ente, secondo la scala definita precedentemente.

Per ogni macro-categoria, viene marcata con una X la misura dell'impatto.

Per ogni macro-categoria, viene aggiunta sempre una adeguata spiegazione che motivi la misura dell'impatto individuata.

Acr	Macro-categoria di rischio	Impatto				Motivazione
		0	1	2	3	
Unah	**Uso non autorizzato dell'hardware** In molti casi i dipendenti possono utilizzare la potenza di calcolo della CPU per propri fini, magari archiviando in memoria dei programmi che vengono richiamati in servizio quando il controllo è meno stretto. La frequenza dei controlli e l'esame dei log di sistema sono determinanti nel rivelare questo tipo di perdite.			X		In questo contesto si inquadra il trattamento non consentito o non conforme di dati personali (violazione dell'art. 167 - illecito penale).
Riin	**Rivelazione illegittima di informazioni anche per negligenza** Il trattamento illecito dei dati è soggetto alle sanzioni previste dal codice penale. L'incaricato dovrebbe essere consapevole che il trattamento dei dati personali è soggetto alla tutela così come previsto dal codice D.lgs. 196/2003, dal codice civile (art. 2050) e dagli specifici articoli del codice penale				X	La rivelazione di informazioni può avere riflessi di triplice natura: penali, finanziari (connessi all'applicazione di sanzioni e risarcimenti), riflessi d'immagine. In Italia, grazie all'entrata in vigore della legge 675/96 e del presente codice, i riflessi che un tempo erano solo civili assumono rilevanza penale, il che significa che non sono sempre monetizzabili.
Anai	**Alterazione non autorizzata di informazioni** Un dipendente od un esterno possono alterare deliberatamente uno o più file del sistema di elaborazione. L'alterazione può avvenire tramite l'accesso ai sistemi per furto di credenziali di autenticazione, l'azione di virus e di codici malefici, lo spamming ed altre tecniche di sabotaggio			X		In questo caso il costo del risarcimento è legato al costo del ricontrollo di tutti i file potenzialmente affetti e non solo da quello eventualmente identificato. Si applicano inoltre sanzioni penali. Il ricontrollo viene fatto, tipicamente, per confronto con i dati cartacei originali, ammesso che essi siano ancora disponibili.
Prin	**Perdita di informazioni** Questa perdita può essere causata da eventi naturali o da atti dolosi o da errori od omissioni.				X	Il risultato finale, in termini di perdita, evidentemente non cambia, anche perché spesso è praticamente impossibile ricostruire con certezza la causa che ha generato una perdita di informazioni. Il costo della perdita è valutabile sulla base dei costi medi di ricostruzione dei dati, in termini di manodopera, di tempo macchina, di attrezzature. Restano impregiudicate le sanzioni penali.
Unai	**Uso non autorizzato di informazioni** Questo sinistro può appartenere ad una delle categorie già esaminate, se non fosse per il ruolo attivo e prolungato del perpetratore. Esso può avvenire in seguito a furto delle credenziali di autenticazione			X		Permette all'intruso di poter accedere ad una stazione di lavoro o ad un server con le autorizzazioni legate alle credenziali sottratte e arrecare qualsiasi tipo di danno ai dati trattati
Unaa	**Uso non autorizzato di applicativi** Permette ad utenti autenticati sul Sistema Informativo di accedere ad informazioni e dati gestite dalle applicazioni, senza la necessità di necessaria autorizzazione			X		Il costo di questo sinistro è difficile da quantizzare e può perfino avere dimensioni tali da portare in fallimento l'Ente; tutto dipende dal tipo di applicativo coinvolto (standard oppure un raffinato programma di gestione). Se si tratta di applicazioni standard, il costo è assimilabile al costo di un utilizzo legittimo dell'applicazione; a tali costi vanno aggiunte le sanzioni penali, ove il trattamento non autorizzato abbia portato a violazioni della legge ed abbia ecceduto i limiti del consenso al trattamento, espresso

						dall'interessato.
Psup	**Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie** In questa categoria si possono includere i supporti magnetici non cancellati, i libri o la documentazione di supporto, i manuali, i nastri per stampante, cassette video, altre attrezzature normalmente utilizzate nei centri EDP, parti di ricambio, strumenti. Restano impregiudicate le sanzioni penali, previste dal regolamento. La perdita o il riutilizzo improprio possono essere causati da atti deliberati (furti), accidentali, negligenza (disordine).			X		In seguito ad un evento di questo tipo, persone estranee possono venire a conoscenza di di dati personali e sensibili presenti sui supporti per cui il danno potrebbe assumere rilevanza molto alta.

5.3 Analisi dei rischi

La tabella seguente sintetizza, per ognuna delle macrocategorie di rischio definite precedentemente, i fattori di rischio che possono risultare critici per la sicurezza dei dati trattati dall'Ente, evidenziando per ciascuno di essi il livello di criticità, ovvero la difficoltà da parte dell'Ente stesso di garantire il non accadimento dell'evento dannoso (la scala di rilevanza è quella a quattro livelli già illustrata):

0 = criticità bassa
1 = criticità media
2 = criticità alta; aspetto importante
3 = criticità molto alta; aspetto fondamentale

I fattori di rischio evidenziati costituiscono il riferimento principale per la definizione di opportune contromisure da adottare che consentano di governare le criticità e di garantire la messa in sicurezza dell'Ente.

Nella colonna "Impatto" viene riportato dal paragrafo precedente l'impatto che ha ciascuna macro-categoria di rischio sulla sicurezza dell'Ente.

Accanto ad ogni fattore di rischio viene marcata con una X la sua criticità nella scala di rilevanza a quattro livelli, motivata adeguatamente.

Acr	Macro-categorie di rischio e fattori di rischio	Impatto				Criticità rilevate nel Comune				
		0	1	2	3	0	1	2	3	Motivazione
Unah	**Uso non autorizzato dell'Hardware**			X						
	Utilizzo potenza di calcolo a propri fini					X				Rischio non elevato nell'Ente
	Furto di credenziali di autenticazione							X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.

	Intercettazione di informazioni in rete		X			Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**			
Riin	**Rivelazione illegittima di informazioni, anche per negligenza**				**X**		
	Comportamenti sleali o fraudolenti		X			Rischio non elevato nell'Ente. In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti.
	Carenza di consapevolezza, disattenzione ed incuria	X				Un atteggiamento negligente, disattento ed inconsapevole può provocare i maggiori danni su ciascun trattamento da parte degli incaricati, non è molto diffuso nell'Ente.
	Intercettazione di informazioni in rete		X			Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**			
Anai	**Alterazione non autorizzata di informazioni**			**X**			
	Furto di credenziali di autenticazione			X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Azioni di virus informatici o codici malefici			X		Dalla rilevazione fatta, si evince che le postazioni di lavoro sono adeguate a fronteggiare tale rischio. E' garantita l'operazione di aggiornamento dei virus su tutte le postazioni di lavoro. Il Comune ha collegato in rete locale tutti i PC ed ha installato un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. Non abbassare la guardia.
	Spamming o altre tecniche di sabotaggio		X			Il Comune ha attivato il servizio di posta elettronica per la maggior parte degli uffici e la PEC per i Responsabili di struttura. Il servizio antispamming è fornito dai provider e dal firewall.
	Errori umani			X		E' sempre possibile commettere errori di digitazione sui dispositivi di input degli strumenti informatici. Devono essere impartite istruzioni agli operatori sulla necessità di verificare sempre l'esattezza dei dati impostati.
	Comportamenti sleali o fraudolenti		X			Rischio non elevato nell'Ente. In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti.

	Accessi esterni non autorizzati		X			L'Ente è al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri. Si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte degli uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un firewall per la protezione della rete LAN e l'antivirus su tutte le macchine.
	Carenza di consapevolezza, disattenzione o incuria			X		Un atteggiamento negligente, disattento ed inconsapevole può provocare danni notevoli. Il Comune deve porre particolare attenzione ad un piano programmato di back-up e recovery riguardante le banche dati delle principali applicazioni informatiche, così da poter ripristinare i dati in caso di alterazione.
	Valore Medio			**X**		
Prin	**Perdita di informazioni**				**X**	
	Azioni di virus informatici o codici malefici			X		Dalla rilevazione fatta, si evince che le postazioni di lavoro sono adeguate a fronteggiare tale rischio. E' garantita l'operazione di aggiornamento dei virus su tutte le postazioni di lavoro. Il Comune ha collegato in rete locale tutti i PC ed ha installato un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. Non abbassare la guardia.
	Spamming o altre tecniche di sabotaggio		X			Il Comune ha attivato il servizio di posta elettronica per la maggior parte degli uffici e la PEC per i Responsabili di struttura. Il servizio antispamming è fornito dai provider e dal firewall.
	Malfunzionamento, indisponibilità o degrado degli strumenti			X		L'Ente ha attivato un piano di adeguamento per mettersi al riparo da questi rischi tramite l'installazione di gruppi di continuità, azioni programmate di back-up e recovery configurate e tenute sotto controllo da un amministratore informatico. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.
	Guasto tecnologico ai sistemi complementari			X		Non sono utilizzati impianti di condizionamento; solo in parte sono utilizzati gruppi di continuità; il sistema elettrico e di collegamento non è canalizzato e differenziato, quindi un corto circuito potrebbe innescare incendi. Esiste un impianto antincendio ed i computer sono sollevati da terra, quindi sono protetti da rischio di allagamento. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.
	Carenza di consapevolezza, disattenzione o incuria		X			Un atteggiamento negligente, disattento ed inconsapevole può provocare danni notevoli. Il Comune ha posto, negli ultimi tempi particolare attenzione ad un piano programmato di back-up e recovery riguardante le banche dati delle principali applicazioni informatiche, così da per poter ripristinare i dati in caso di alterazione.
	Errori umani		X			E' sempre possibile commettere errori di digitazione sui dispositivi di input degli strumenti informatici. E' necessario impartire le dovute istruzioni agli operatori che trattano direttamente o indirettamente con gli strumenti elettronici.
	Asportazione e furto di strumenti contenenti dati		X			L'accesso ai locali è controllato, le porte e i balconi maggiormente accessibili, perché a piano terra, sono dotati di inferriate. E' stato istituito un luogo sicuro dove conservare i supporti di back-up relativi alle banche dati delle applicazioni sw gestite.
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria			X		Il Comune ha installato e mantiene un impianto antincendio; ha provveduto a sollevare i PC da terra contro il rischio di allagamento. Occorre fronteggiare ulteriormente il rischio attuando il Piano di Disaster & Recovery e Continuità Operativa.
	Valore Medio			**X**		

Unai	**Uso non autorizzato di informazioni**				X	
	Furto di credenziali di autenticazione per l'accesso ad un computer e/o alle applicazioni censite			X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Comportamenti sleali o fraudolenti	X				In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti. Non abbassare la guardia
	Accessi esterni non autorizzati		X			L'Ente è parzialmente al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri. Occorre dare istruzioni precise al guardiano fisso all'ingresso; si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte di uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un firewall per la protezione della rete LAN.
	Intercettazione di informazioni in rete		X			Le applicazione sw utilizzate e le rispettive banche dati sono meno esposte ad eventuali accessi dalla rete e relative intercettazioni, perché il Comune ha provveduto al collegamento in rete delle stazioni di lavoro degli incaricati ed alla messa in protezione della rete, anche tramite firewall; in tal modo la rete dati interna (LAN) è separata dal mondo esterno (WAN). Stabilire le regole di sicurezza per l'uso della posta elettronica ed internet e formare il personale.
	Valore Medio		**X**			
Unaa	**Uso non autorizzato di applicativi**				X	
	Furto di credenziali di autenticazione per l'accesso alle applicazioni censite			X		L'utilizzo delle credenziali di accesso (ID e Password) è strettamente riservato agli incaricati del trattamento. E' sempre meno frequente l'utilizzo da parte di più utenti delle medesime credenziali di accesso per accedere alle applicazioni software rilevate. La loro custodia deve essere garantita dai responsabili dei singoli servizi. Occorre regolamentare la procedura di gestione delle credenziali di autenticazione.
	Comportamenti sleali o fraudolenti		X			In qualche caso gli incaricati del trattamento potrebbero non essere consapevoli della gravità di tali azioni. L'Amministrazione comunale programma attività di aggiornamento periodico del personale incaricato ai trattamenti. Non abbassare la guardia
	Accessi esterni non autorizzati		X			L'Ente è parzialmente al riparo da accessi esterni non autorizzati di tipo fisico, avendo istituito nella sede principale il controllo degli accessi tramite uscieri; nella sede destinata ai Servizi Sociali il portone d'ingresso viene tenuto chiuso ed è necessario bussare per potervi accedere. Occorre dare istruzioni precise al guardiano fisso all'ingresso; si potrebbe istituire un registro degli accessi. Il Comune ha sostituito le serrature delle porte di uffici che trattano dati sensibili con serrature a norma europea. Per quanto riguarda le misure di protezione di tipo logico è stato configurato un proxy server Linux per la protezione della rete LAN.
	Valore Medio		**X**			

Psup	**Perdita o riutilizzo di supporti cartacei o magnetici o documentazioni accessorie**			X			
	Malfunzionamento, indisponibilità o degrado degli strumenti			X		L'Ente ha attivato un piano di adeguamento per mettersi al riparo da questi rischi tramite l'installazione di gruppi di continuità, azioni programmate di back-up e recovery configurate e tenute sotto controllo da un amministratore informatico. Non è stato attuato il Piano di Disaster & Recovery e Continuità Operativa approvato dalla ex DigitPA.	
	Carenza di consapevolezza, disattenzione o incuria	X				E' presente nell'Ente un atteggiamento consapevole sulle regole di mantenimento dei supporti magnetici ed ottici.	
	Asportazione e furto di strumenti contenenti dati		X			L'accesso ai locali è controllato, le porte e i balconi maggiormente accessibili, perché a piano terra, sono dotati di inferriate. E' stato istituito un luogo sicuro dove conservare i supporti di back-up relativi alle banche dati delle applicazioni sw gestite.	
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria			X		Il Comune ha installato e mantiene un impianto antincendio; ha provveduto a sollevare i PC da terra contro il rischio di allagamento. Occorre fronteggiare ulteriormente il rischio attuando il Piano di Disaster & Recovery e Continuità Operativa.	
	Valore Medio		X				

Legenda:

IMPATTO: 0= impatto basso; 1= impatto medio; 2=impatto alto, aspetto importante; 3= impatto molto alto; aspetto fondamentale

CRITICITA': 0= criticità basso; 1= criticità medio; 2= criticità alto, aspetto importante; 3= criticità molto alto; aspetto fondamentale

5.4 Sintesi dei rischi

Il grafico seguente sintetizza il livello di rischio rispetto agli aspetti analizzati in precedenza.

Nella tabella seguente si riporta l'acronimo del relativo aspetto analizzato nelle tabelle impatto precedenti (es. Unah: Uso non autorizzato dell'hardware) nella posizione intercettata dal valore dell'impatto identificato, con il valore medio dei relativi fattori di rischio analizzati nella tabella analisi del rischio.

Legenda:

Unah: Uso non autorizzato hw
Riin: Rivelazione illegittima di Informazioni , anche per negligenza
Anai: Alterazione non autorizzata di Informazioni
Prin: Perdita di informazioni
Unai:Uso non autorizzato di informazioni
Unaa: Uso non autorizzato di applicativi
Psup: Perdita o riutilizzo di supporti cartacei o magnetici o

Area Critica

Impatto				
3		Riin	**Prin**	
2		Unai Unaa Unah Psup	**Anai**	
1				
0				
	0	1	2	3

Criticità

documentazioni accessorie

6 Piano di adeguamento

In questo capitolo viene presentato il piano di adeguamento adottato dalla AOO a seguito dell'analisi dei rischi effettuata, in termini di:

- misure di sicurezza adottate
- misure di sicurezza da adottare

Nella tabella seguente si riporta una sintesi degli aspetti critici per la sicurezza dell'Ente e vengono, inoltre, indicati i trattamenti, o contromisure da adottare, per fronteggiare e mantenere sotto controllo ciascuna di tali criticità.

La tabella che segue costituisce la sintesi dell' analisi dei rischi effettuata ed è molto importante perché riassume tutte le principali azioni da intraprendere per raggiungere il traguardo della protezione dei documenti trattati dall'Ente e dei dati personali in essi contenuti.

Misure di sicurezza adottate e da adottare

Macro categoria di rischio	Fattore di rischio	Misure in essere	Misure da adottare	Priorità	Tipo di adeguamento
ANAI	•Furto di credenziali di autenticazione	Il comune ha realizzato un progetto per la configurazione completa della rete e, quindi, gli incaricati sono dotati di credenziali di autenticazione per l'accesso alla rete. Le credenziali di autenticazione rispondono ai requisiti richiesti dal D.Lgs. 196/03 – Allegato B.	Occorre incaricare un custode delle password e predisporre istruzioni operative sull'uso corretto delle credenziali. L'Amministrazione comunale ha programmato un corso di formazione agli incaricati che sarà erogato nell'anno in corso.	Massima	Logico Organizzativo
PRIN ANAI	•Carenza di consapevolezza, disattenzione o incuria •Errori umani		Programmare interventi di formazione e/o informazione agli incaricati sulla sicurezza dei dati, estesi anche alle tecnologie ed applicazioni in uso presso l'Ente. Predisporre, adottare e distribuire linee guida, procedure organizzative, mansionari ed informativa ai dipendenti.	Alta	Organizzativo
PRIN	•Malfunzionamento, indisponibilità o degrado degli strumenti	Esiste contratto di manutenzione attivo con le Ditte fornitrici delle applicazioni sw. E' stato attivato un supporto di assistenza e manutenzione dell'infrastruttura di comunicazione e degli strumenti. E' stato affidato l'incarico di amministratore informatico ad un tecnico esterno che garantisce la disponibilità dei dati tramite un adeguato programma di back up e recovery.	Occorre che il responsabile informatico continui nelle azioni di organizzazione, controllo e garanzia sulla piena disponibilità dei dati, sul buon funzionamento degli strumenti di sicurezza installati, della rete e di tutta la strumentazione hw e sw configurata in rete. Il responsabile informatico deve garantire il tracciamento degli accessi dell'amministratore di sistema e controllarne l'operato periodicamente. Occorre attuare il piano di disaster & recovery e continuità operativa.	Alta	Logico, fisico ed organizzativo
ANAI	•Comportamenti sleali o fraudolenti	E' stato installato un firewall che permette il tracciamento di qualsiasi tentativo di intrusione sulla rete LAN del Comune.	Proteggere documenti con dati sensibili e giudiziari salvandoli in modo criptato.	Alta	Organizzativo e logico

		Sono state attivate firma digitale e posta elettronica certificata sui documenti elettronici con validità probatoria.			
PRIN	•Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	I computer sono protetti da allagamenti, perché installati su un carrellino e quindi sollevati da terra. E' stato installato e viene verificato periodicamente l'impianto antincendio ai sensi della L. 626/94. Viene effettuato il back up giornaliero delle banche dati. E' stato predisposto un piano di disaster & recovery e continuità operativa su cui la ex DigitPA ha espresso parere favorevole.	Occorre destinare un luogo sicuro (ad es. cassaforte ignifuga posta in un luogo sicuro lontano dalla sede del server) per la conservazione dei supporti su cui vengono salvati i dati. Occorre passare all'attuazione del piano di disaster & recovery e continuità operativa.	Alta	Logico Organizzativo
PRIN	•Guasto tecnologico ai sistemi complementari	Sono stati installati i gruppi di continuità su tutti i server e le postazioni di lavoro.	Rafforzare le misure di protezione ai sistemi informativi, adeguando tali sistemi con dispositivi di allarme che possano prevenire gravi conseguenze agli strumenti elettronici ospitati. Attuare il Piano di Disaster & Recovery e Continuità Operativa	Alta	Fisico
PRIN ANAI	•Azioni di virus informatici o codici malefici su strumenti connessi e non alla rete	Il Comune ha realizzato un progetto per il collegamento in rete di tutti i PC e l'installazione di un antivirus centralizzato sul server che aggiorna quotidianamente tutte le postazioni di lavoro del Comune. E' stato incaricato un amministratore informatico che ha la responsabilità di garantire il buon funzionamento dei servizi in oggetto.	Stabilire idonee politiche di sicurezza per ciò che riguarda l'aggiornamento delle patch di Microsoft che non risultano sempre aggiornate sulle postazioni di lavoro.	Media	Logico
ANAI PRIN	•Accessi esterni non autorizzati •Asportazione e furto di strumenti contenenti dati	La sede principale è dotata di guardiania e l'ingresso agli uffici da parte di persone estranee è controllato strettamente. Le finestre e i balconi situati a piano terra sono protetti da inferriate. Le porte degli uffici sono state dotate di serrature idonee e funzionanti.	Attuare il Piano di Disaster & Recovery e Continuità Operativa	Bassa	Fisico

Nella tabella seguente si effettua, per ogni macro-categoria di rischio, una valutazione dell'impatto che hanno le relative contromisure da adottare sui tre tipi di adeguamento:

- logico
- organizzativo
- fisico

La valutazione deriva anche dalle motivazioni espresse nell'analisi dei rischi.

Macro categoria di rischio	Impatto		
	Adeguamento Logico	Adeguamento Organizzativo	Adeguamento Fisico

Macro categoria di rischio	Impatto		
	Adeguamento Logico	Adeguamento Organizzativo	Adeguamento Fisico
PRIN: Perdita di Informazioni	**3**	2	0
ANAI: Alterazione non autorizzata di informazioni	**1**	**2**	0

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Piano di formazione
per il personale dell'Amministrazione

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato viene riportato il programma di formazione rivolto al personale dipendente.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 PREMESSA

Per la buona riuscita del progetto di attuazione del Manuale per la Gestione documentale, occorre porre particolare attenzione alle necessità formative delle varie categorie di personale coinvolto nei processi di gestione informatica dei documenti.

Chiunque si occupi di informatica sa bene che uno dei principali servizi destinati agli utenti del sistema, anche se spesso trascurato, è la formazione degli operatori. E' illuminante l'esperienza di tanti enti o aziende che hanno acquistato sofisticati programmi applicativi e ne hanno verificato la scarsa efficacia, perché il personale non li sapeva utilizzare in modo appropriato.

Pertanto, la messa a punto di un piano di formazione è essenziale per garantire all'Ente di evolversi e di rafforzarsi, rendendo più sicure le modalità di utilizzo, più rapido il lavoro e più affidabile e razionale l'organizzazione.

2 OBIETTIVI DELL'INTERVENTO FORMATVO

L'intervento si propone di realizzare un piano di addestramento e formazione per il personale comunale al fine di metterlo nelle condizioni di utilizzare senza problemi l'infrastruttura tecnologica e la piattaforma software di supporto alla gestione dei documenti.

3 PROGRAMMA DI FORMAZIONE

Coerentemente con i contenuti del presente Manuale per la Gestione documentale, il programma formativo prevede tre modalità differenti di formazione:

1. sessioni di formazione teorica erogate tramite lezioni d'aula;
2. sessioni pratiche sull'utilizzo delle funzionalità dei programmi applicativi (protocollo, atti amministrativi, procedimenti, carteggi, fascicoli, contratti, archivio documentale, ecc.)
3. sessioni di formazione a distanza;

Sono previsti più moduli formativi ognuno dei quali si focalizza su uno dei seguenti argomenti:

- trattamento informatico dei documenti
  - flussi dei documenti in entrata
  - flussi dei documenti in uscita
  - flussi dei documenti interni
  - protocollazione
  - titolario di classificazione
  - fascicolazione dei documenti
  - archiviazione e conservazione
- Lezioni dedicate alle procedure organizzative ed istruzioni operative adottate nel Manuale per la gestione documentale, quali ad esempio:
  - PO - Uso della posta elettronica certificata e tradizionale
  - PO - Sottoscrizione documenti informatici

- IO - Formati elettronici dei documenti informatici

- Lezioni dedicate alle procedure sw in uso presso l'Ente
  - gestione del protocollo informatico, la classificazione e la fascicolazione dei documenti
  - gestione degli atti amministrativi e messi notificatori
  - gestione dei carteggi, fascicoli, e procedimenti
  - gestione dotazione organica e gestione dei contratti
  - sistema per la gestione dell'archivio documentale
- Piano di sicurezza

4 TEMPI DI ATTUAZIONE

L'attuazione del programma formativo è pianificata per l'anno in corso.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Piano di conservazione

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato viene riportato uno schema di massimario di selezione e scarto che l'Amministrazione dell'Ente può utilizzare come guida alla predisposizione del proprio.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 PIANO DI CONSERVAZIONE

Di seguito viene proposto uno schema di massimario di selezione e scarto per Enti comunali che può essere utilizzato come guida. Lo schema di esempio riportato è quello predisposto dal CNIPA a febbraio 2006, pubblicato sulla rivista “i Quaderni” n. 21.

1.1 Documentazione da conservare senza limiti di tempo

- Atti delle Commissioni elettorali mandamentali concernenti la presentazione delle candidature;
- Atti e documenti del contenzioso legale;
- Atti relativi ai lavori pubblici, eseguiti e non eseguiti, limitatamente a originali dei progetti e dei loro allegati, perizie di spesa, libri delle misure;
- Bilanci e consuntivi originali (o nell’unica copia esistente);
- Contratti;
- Corrispondenza generale del servizio esattoria e tesoreria;
- Corrispondenza, salvo quanto indicato nella seconda parte;
- Deliberazioni destinate a formare la raccolta ufficiale del Consiglio e della Giunta;
- Documentazione generale per la richiesta di mutui, anche estinti;
- Elenchi dei poveri;
- Fascicoli degli amministratori e dei membri delle commissioni;
- Fascicoli del personale in servizio e in quiescenza, di ruolo e non di ruolo;
- Inventari dei beni mobili e immobili del Comune;
- Inventari, schedari, rubriche e repertori dell’archivio, libretti o schede di trasmissione di carte tra i vari uffici, anche non più in uso;
- Libri contabili obbligatori in base alle leggi fiscali;
- Libri infortuni o documentazione equivalente;
- Libri mastri, libri giornale, verbali di chiusura dell’esercizio finanziario;
- Liste di leva e dei renitenti;
- Ordinanze e circolari del Comune;
- Originali dei verbali delle Commissioni di concorso;
- Piani commerciali, licenze e autorizzazioni amministrative all’esercizio del commercio fisso;
- Piani regolatori generali e particolareggiati; piani delle lottizzazioni; regolamenti edilizi; licenze, concessioni e autorizzazioni edilizie;
- Posizioni previdenziali, stipendiali, tributarie dei dipendenti quando non integralmente conservate nei fascicoli personali;
- Programmi pluriennali di attuazione e piani di suddivisione in lotti delle aree suscettibili di attività estrattiva;
- Protocolli della corrispondenza;
- Qualunque atto o documento per il quale una legge speciale imponga la conservazione illimitata;
- Registri dei verbali e protocolli delle Commissioni comunali;
- Registro della popolazione comprensivo dei fogli di famiglia eliminati, registri e specchi riassuntivi del movimento della popolazione;
- Regolamenti e capitolati d’oneri;
- Rilevazioni di carattere statistico non pubblicate;

- Ruoli delle imposte comunali;
- Ruoli matricolari;
- Ruoli riassuntivi del personale e Libri matricola;

- Tariffe delle imposte di consumo e delle altre tasse riscosse a tariffa;
- Verbali delle aste;
- Verbali delle Commissioni elettorali;
- Verbali di sezione per l'elezione dei consigli comunali e dei consigli circoscrizionali.

1.2 Documentazione eliminabile dopo cinque anni

- Annotazioni marginali eseguite agli atti di stato civile provenienti da altri comuni e altre assicurazioni di trascrizione relative agli stessi;
- Atti relativi a concorsi a borse di studio e premi (conservando la seguente documentazione: originale degli atti della Commissione o dei comitati, gli eventuali rendiconti speciali, una copia degli stampati e dei manifesti, il registro delle opere esposte in occasione di mostre artistiche e simili);
- Atti relativi alla costituzione e all'arredamento dei seggi (conservando il prospetto delle sezioni e della loro ubicazione);
- Atti relativi alla regolamentazione della propaganda (conservando la documentazione riassuntiva;
- Atti relativi all'orario degli ambulatori;
- Atti relativi all'organizzazione di censimenti;
- Atti rimessi da altri Enti per l'affissione all'albo;
- Atti rimessi da altri Enti per notifiche;
- Autorizzazioni all'uso di impianti culturali e sportivi (conservando eventuali atti riassuntivi);
- Avvisi di convocazione delle Commissioni;
- Bollettari di prelevamento oggetti dall'Economato;
- Bollettari di ricevute dell'esattoria;
- Brogliacci di viaggio degli automezzi comunali;
- Carteggi per la richiesta di atti notori e di certificati diversi con eventuale copia degli stessi;
- Carteggio interlocutorio per la concessione in uso di locali e oggetti di proprietà comunale;
- Carteggio relativo alla contabilità per registri di stato civile (conservando le fatture per dieci anni);
- Certificazioni per richieste ai fini della fruizione di assegni di studio;
- Circolari per l'orario degli uffici e per il funzionamento degli uffici;
- Comunicazioni relative a variazioni anagrafiche;
- Consiglio regionale e provinciale - Carteggio con gli uffici militari per aggiornamento di ruoli;
- Consiglio regionale e provinciale - Carteggio tra comuni per l'aggiornamento dei ruoli matricolari;
- Consiglio regionale e provinciale - Matrici di richieste di congedi anticipati;
- Consiglio regionale e provinciale - Verbali dell'Ufficio centrale circoscrizionale relativi al completamento delle operazioni elettorali;
- Consiglio regionale e provinciale - Verbali sezionali privi di allegati (comunque non prima della decisione di eventuali ricorsi);
- Conto dell'Economato (conservando eventuali prospetti generali);

- Copia di deliberazioni per liquidazione indennità alla Commissione elettorale mandamentale e ad altre commissioni non comunali;
- Copia di delibere per pagamento di gettoni di presenza ai partecipanti alle commissioni;
- Copia di lettere di trasmissione di denunce di malattie infettive;
- Copie degli elenchi dei buoni libro concessi e documentazione di supporto (conservando l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali; eventuali fatture dovranno essere conservate per dieci anni);
- Copie degli inviti agli utenti convocati per la verifica biennale dei pesi e delle misure per altri adempimenti;
- Copie delle comunicazioni delle sezioni relative ai dati parziali sul numero dei votanti (conservando eventualmente la copia dei fonogrammi trasmessi per l'insieme delle sezioni);
- Copie di attestati di servizio;
- Copie di atti giudiziari notificati dal Comune;
- Copie di atti notori;
- Copie di deliberazioni per contributi assistenziali diversi (conservando le richieste le proposte);
- Copie di deliberazioni per contributi ad enti e associazioni diverse (conservando le richieste);
- Copie di delibere di liquidazione di contributi per concerti, attività culturali, biblioteca comunale, biblioteche scolastiche (conservando la corrispondenza o la richiesta, una copia dei programmi e dei manifesti e gli elenchi dei libri forniti);
- Copie di delibere di liquidazioni dei compensi al personale straordinario per corsi serali e carteggio transitorio sui corsi (conservando gli atti di interesse per il personale che ha prestato servizio e relazioni finali, programmi di spesa, altri documenti riassuntivi);
- Copie di istruzioni a stampa (conservandone una per ciascuna elezione);
- Copie e minute dei progetti, sia realizzati che non realizzati;
- Corrispondenza interlocutoria per commemorazioni e solennità civili (conservando carteggi generali per l'organizzazione delle manifestazioni, una copia degli inviti, degli stampati e dei manifesti, gli atti dei comitati, eventuali rendiconti particolari ed eventuali fatture per dieci anni);
- Corrispondenza per la richiesta di licenze di pubblica sicurezza o rilasciate da altri uffici;
- Corrispondenza per la richiesta e la trasmissione di certificati di esito di leva;
- Corrispondenza relativa alla formazione delle schede personali, alle aggiunte o alle cancellazioni dalle liste;
- Delegazioni alla celebrazione di matrimonio in altri comuni;
- Documenti di carico e scarico dei bollettari delle imposte;
- Domande di allacciamento all'acquedotto e richieste di concessione di illuminazione, ove le stesse non facciano fede di contratto (in tal caso saranno eliminabili cinque anni dopo l'esaurimento del contratto);
- Domande di commercianti per deroghe all'orario dei negozi;
- Domande di occupazione temporanea di spazi ed aree pubbliche per fiere, mostre, comizi, feste (conservando quelle relative a concessioni permanenti [p.es. passi carrabili] per quarant'anni ed eventuali registri indefinitamente);
- Domande di partecipazione alla Befana e ad altre elargizioni;
- Domande per la concessione dei libretti di lavoro e libretti restituiti al Comune;
- Domande per la richiesta di certificati, carteggi per la loro trasmissione;
- Domande per pubbliche affissioni (conservando le pratiche che hanno dato luogo a contenzioso);

- Elenchi dei turni di servizio della Polizia municipale (conservando i regolamenti);
- Elezioni dei deputati alla costituente - Verbali degli uffici centrali di circoscrizione concernenti il completamento delle operazioni di votazione;
- Elezioni dei deputati alla costituente - Verbali sezionali con allegati;
- Elezioni della Camera e del Senato - Carteggio relativo alla designazione dei rappresentanti di lista presso gli uffici di sezione, dal 1976;
- Elezioni della Camera e del Senato - Verbali degli uffici centrali di circoscrizione per il completamento delle operazioni;
- Elezioni della Camera e del Senato - Verbali sezionali, privi di allegati;
- Estratti dei verbali dell'Ufficio centrale circoscrizionale relativi al riesame di voti contestati;
- Fascicoli e schede personali dei giudici popolari;
- Fascicoli e schede personali di cittadini cancellati dalle liste per morte o emigrazione;
- Lettere di rifiuto di partecipazione alle aste, offerte di ditte non prescelte;
- Lettere di trasmissione di carte d'identità;
- Lettere di trasmissione di passaporti; autorizzazioni alla richiesta degli stessi;
- Libretti dei veicoli;
- Liste dei giudici popolari;
- Liste sezionali se esistono le liste generali;
- Matrici dei certificati elettorali in bianco e non consegnati;
- Matrici delle proposte di annotazioni marginali inviate alle Procure;
- Matrici di bollettari per acquisto materiali di consumo per l'ufficio tecnico;
- Matrici di buoni di acquisto generi di refezione e comunque di consumo;
- Matrici o copie di comunicazioni anagrafiche ad altri uffici comunali;
- Moduli per l'accertamento al diritto del trasporto gratuito degli alunni (conservando eventuali relazioni riassuntive);
- Note di frequenza, ricevute di pagamento di rette e domande di esonero per scuole materne (conservando gli elenchi dei beneficiati; eventuali fatture dovranno essere conservate per dieci anni);
- Parlamento europeo - Carteggi relativi alle designazioni dei rappresentanti di lista presso gli uffici di sezione (conservando eventualmente la documentazione contenente dati più generali);
- Parlamento europeo - Estratti del verbale dell'Ufficio elettorale provinciale per il riesame delle schede di voti contestati (non prima della decisione c.s.);
- Parlamento europeo - Verbali dell'Ufficio elettorale provinciale per il riesame delle schede di voti contestati (non prima della decisione c.s.);
- Parlamento europeo - Verbali dell'Ufficio provinciale relativi al completamento di operazioni;
- Parlamento europeo - Verbali sezionali privi di allegati (non prima della decisione di eventuali ricorsi previsti dagli artt. 42 e 43 della L. 24 gennaio 1979, n. 18);
- Prospetti dei lavori eseguiti dai cantonieri;
- Prospetti di carattere pubblicitario, richiesti e non richiesti, preventivi di massima non utilizzati;
- Referendum abrogativi - Carteggio relativo alla designazione dei rappresentanti dei partiti e dei gruppi politici e dei comitati promotori presso le sezioni (conservando eventualmente la documentazione contenente dati generali);
- Referendum abrogativi - Estratti del verbale dell'Ufficio provinciale per il referendum relativo al riesame dei voti contestati e provvisoriamente non assegnati, per ogni sezione;

- Referendum abrogativi - Verbali di completamento dello spoglio delle schede eseguito da parte dell'Ufficio provinciale per il Referendum;
- Referendum abrogativi - Verbali sezionali privi di allegati;
- Referendum istituzionale - Verbali degli uffici centrali circoscrizionali concernenti il completamento delle operazioni di votazione.
- Referendum istituzionale - Verbali sezionali con allegati;
- Registri e bollettari di spese postali;
- Registro di carico e scarico dei bollettari;
- Richiesta di invio di notizie varie relative ai militari (esclusi i periodi bellici);
- Rubriche interne per il calcolo dei congedi e delle aspettative;
- Scadenzari dell'Ufficio elettorale per la compilazione delle liste;
- Schede personali dei giovani compresi nella leva di altri comuni o deceduti prima della stessa;
- Schede personali dei militari da includere nella lista di leva;
- Solleciti di pagamento fatture pervenuti al Comune;
- Stampati e circolari per campagne nazionali di lotta contro le malattie;
- Tabelle provvisorie delle preferenze non costituenti verbale;
- Telegrammi della Prefettura per l'esposizione della bandiera nazionale conservando le ordinanze e gli avvisi del sindaco;
- Verbali di consegna di materiale elettorale; verbali di controllo dei verbali sezionali per l'accertamento che non vi siano fogli in bianco;
- Visite fiscali dei dipendenti comunali e diverse.

1.3 Documentazione eliminabile dopo sette anni

- Fogli di lavoro straordinario (conservando eventuali prospetti riassuntivi);
- Fogli di presenza dei dipendenti;
- Modelli 740 (copia per il Comune); i sette anni decorrono dall'anno cui si applica la dichiarazione.

1.4 Documentazione eliminabile dopo dieci anni

- Atti dei concorsi: copie dei verbali della Commissione giudicatrice;
- Atti di liquidazioni di lavoro straordinario per elezioni;
- Atti relativi a liquidazione di spese "a calcolo";
- Atti relativi a liquidazione di spese di rappresentanza;
- Atti relativi al riparto dei diritti di segreteria e stato civile, sanitari e tecnici;
- Atti relativi all'acquisto di autoveicoli e alla loro manutenzione, con dépliant pubblicitari (conservando proposte di spesa, verbali d'asta, contratti);
- Atti relativi all'alienazione di mobili fuori uso e di oggetti vari;
- Atti relativi alle contravvenzioni sanitarie (conservando i registri, se esistenti);
- Autorizzazioni al trasporto di salme fuori del comune;
- Avvisi di pagamento per compartecipazione di imposte erariali a favore del comune;
- Bollettari di riscossione delle imposte di consumo e delle sue contravvenzioni (conservando i registri e i prospetti delle contravvenzioni);
- Bollettari per la riscossione delle contravvenzioni;
- Bollettari per la riscossione dell'imposta sulla pubblicità, pubbliche affissioni e occupazione di suolo pubblico;

- Carteggi di liquidazione delle missioni ai dipendenti e agli amministratori, con relative tabelle di missione e documentazione allegata, salvo, se esistenti, prospetti generali;
- Carteggi di ordinaria e straordinaria manutenzione delle scuole (conservando proposte di spesa, contratti, verbali d'asta e progetti originali);
- Carteggi per acquisto di vestiario per specifiche categorie di dipendenti (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per acquisto di attrezzature varie, di mobili e di materiale di cancelleria e pulizia per uffici (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per acquisto di macchine d'ufficio e di materiale per la loro manutenzione e per la cancelleria (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per la fornitura di combustibile per riscaldamento (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per l'acquisto di carburante per gli automezzi (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per l'acquisto di materiali per l'Ufficio tecnico e il magazzino comunale (conservando proposte di spesa, verbali d'asta, contratti);
- Carteggi per l'organizzazione della leva, locali e arredamento, materiali, cancelleria (conservando i contratti relativi a forniture);
- Carteggi per pulizia di locali (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi relativi a ordinaria e straordinaria manutenzione di sedi di uffici giudiziari o carceri, (conservando proposte di spesa, progetti originali, verbali d'asta e contratti);
- Carteggi relativi a sottoscrizione di abbonamenti a giornali e riviste e ad acquisto di pubblicazioni amministrative;
- Carteggi relativi all'acquisto di materiali di consumo (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi relativi all'acquisto di materiali per illuminazione pubblica, segnaletica stradale, manutenzione di giardini, piazze, vie, argini dei fiumi, fognature;
- Carteggio interlocutorio e copia di atti per mutui estinti ed accettazioni di eredità;
- Carteggio interlocutorio relativo alle associazioni di comuni;
- Carteggio vario transitorio con le farmacie comunali;
- Cartelle personali dei contribuenti cessati (conservando i ruoli);
- Cartellini delle carte d'identità scadute e carte scadute e restituite al Comune (caso per caso, i carteggi ad esso relativi);
- Copie dei mandati e delle reversali e dei loro allegati;
- Copie dei preventivi e dei consuntivi (conservando il progetto del bilancio);
- Copie di atti per lavori ai cimiteri (conservando l'originale del progetto, i verbali d'asta, i contratti, il conto finale dei lavori e tutti i documenti originali);
- Copie di avvisi per esumazione di salme nei cimiteri (conservando per almeno 40 anni il registro delle lettere spedite e degli avvisi consegnati);
- Corrispondenza relativa al personale del Consiglio e delle Commissioni e alla liquidazione dei loro compensi;
- Denunce mediche di malattie contagiose a carattere non epidemico se trasmesse ad altri uffici;
- Domande di ammissione a colonie;
- Domande di concessione di sussidi straordinari;
- Domande di iscrizione all'elenco dei poveri (conservando l'elenco);

- Domande di partecipazione (conservando per 40 anni i diplomi originali di studio e/o i documenti militari); copie di manifesti inviate ad altri enti e restituite; elaborati scritti e pratici; copie di avvisi diversi; copie di delibere;
- Domande e certificazioni di ditte per essere incluse nell'Albo degli appaltatori comunali;
- Fatture liquidate;
- Inviti alle sedute del Consiglio e della Giunta (conservando gli ordini del giorno con elenco dei destinatari, i fascicoli delle interpellanze ed eventuali progetti e relazioni); mancanza di questi, le loro copie;
- Matrici dei permessi di seppellimento;
- Matrici delle imposte;
- Ordini di sequestro di medicinali in commercio eseguiti su direttive superiori;
- Registri delle riscossioni dei diritti di segreteria e stato civile (conservando eventuali prospetti riassuntivi annuali);
- Richieste di informazioni da parte di ospedali ed enti assistenziali;
- Schedari delle imposte;
- Stati di avanzamento di lavori pubblici;
- Verbali delle contravvenzioni di polizia (conservando i registri);
- Verbali di interramento di animali inadatti all'alimentazione;
- Verbali sezionali dei referendum abrogativi;
- Verifiche di cassa dell'imposta di consumo e registro di carico e scarico dei suoi bollettari.

1.5 Documentazione eliminabile dopo quarant'anni

- Diplomi originali di studio o militari conservati nella documentazione relativa ai concorsi, eventualmente eliminabili prima dei quarant'anni previa emanazione di un'ordinanza con intimazione al ritiro;
- Domande relative a concessioni permanenti;
- Registri degli atti notificati per altri uffici;
- Registro delle lettere spedite agli eredi per esumazione di salme nei cimiteri;
- Matricole delle imposte.

1.6 Documentazione eliminabile dopo cinquant'anni

- Mandati di pagamento e riscossione (comprese le eventuali fatture e le cosiddette "pezze d'appoggio", ma conservando l'eventuale carteggio originale come relazioni, perizie, ecc. che talvolta è rimasto allegato al mandato).

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Procedura organizzativa
Aree Organizzative Omogenee ed Organizzazione

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: La presente guida riporta informazioni sulle Aree Organizzative Omogenee individuate dall'Amministrazione e descrive la struttura organizzativa dell'Ente.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 SCOPO

La presente guida riporta informazioni sulle Aree Organizzative Omogenee individuate dall'Amministrazione e descrive la struttura organizzativa dell'Ente.

1.1 Applicabilità

Il documento è applicabile alla specifica realtà del Comune di Arpaise.

1.2 Aree oggetto dell'intervento

Sono interessate tutte le Unità Organizzative di Riferimento dell'Ente.

1.3 Normativa di riferimento

L'art. 50, comma 4, del DPR 445/00 stabilisce che all'interno di ciascuna amministrazione siano create delle Aree Organizzative Omogenee, in modo da assicurare criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna delle stesse.

L'art. 61 del DPR 445/00 stabilisce, altresì, che si costituisca per ciascuna AOO un Servizio responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al detto Servizio deve essere preposto un dirigente ovvero funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica.

L'art. 3 del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico" ribadisce l'obbligo di individuare le suddette Aree Organizzative Omogenee e di nominare, al loro interno, un Responsabile della gestione documentale nonché un suo vicario per casi di vacanza, assenza o impedimento.

Inoltre, l'Art. 57-bis del CAD istituisce l'indice degli indirizzi della pubblica amministrazione (IPA) e dei gestori di pubblici servizi, nel quale sono indicati gli indirizzi di posta elettronica certificata da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi ed i privati. Le amministrazioni sono tenute ad aggiornare gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale.

2 AREE ORGANIZZATIVE OMOGENEE

Questa amministrazione ha individuato un'unica Area Organizzativa Omogenea denominata "Comune di Arpaise" che è composta dall'insieme di tutti i suoi Uffici Organizzativi la cui articolazione è presentata nei capitoli successivi.

3 ACCREDITAMENTO PRESSO L'IPA

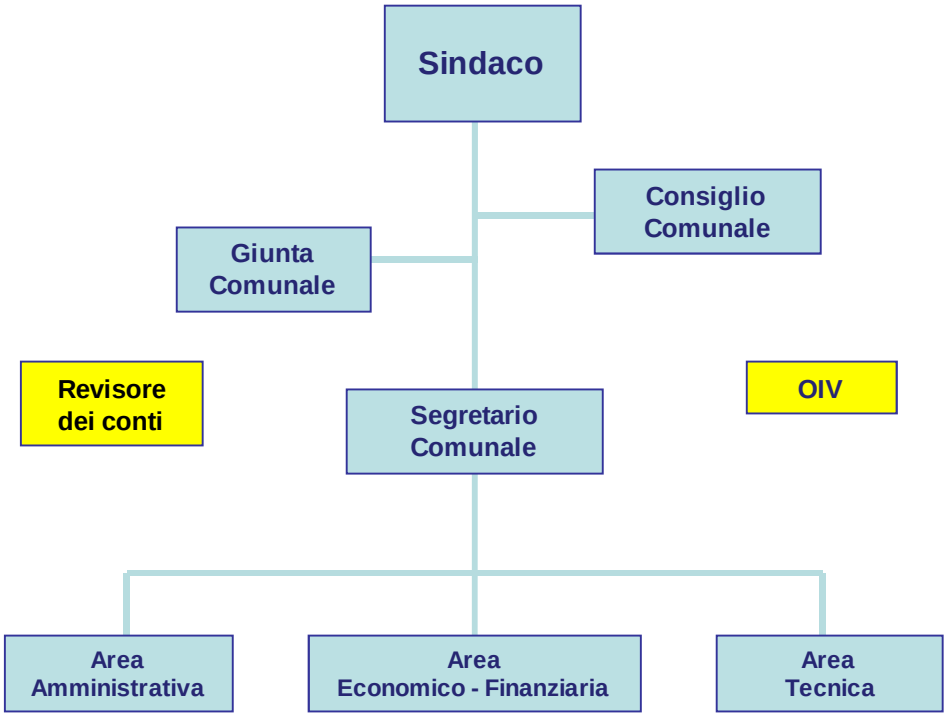
Ai sensi dell' art. 57-bis del CAD, l'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico dall'Agenzia per l'Innovazione Digitale (ex DigitPA), fornendo le seguenti informazioni che individuano l'amministrazione/AOO:

Denominazione dell'Amministrazione	Comune di Arpaise.
Indirizzo della sede principale dell'Amministrazione	Via P.E.Capone - 82010 Arpaise (BN)
Sito istituzionale dell'Ente	www.comunearpaise.it
Casella di posta elettronica istituzionale	comunearpaise@asmepec.it
Denominazione AOO	Comune di Arpaise
Codice identificativo AOO (Codice IPA)	c_a432
Casella di posta elettronica associata alla AOO	comunearpaise@asmepec.it
Data di accreditamento IPA	19/07/2011
Nominativo del referente	Filomena Laudato

Gli Uffici Organizzativi di riferimento sono quelli descritti nel capitolo successivo.

4 ORGANIZZAZIONE DEGLI UFFICI E DEI SERVIZI

Il Comune di Arpaise è organizzato come nella rappresentazione grafica che segue:



Esso opera con l'intento di rappresentare la comunità locale, di promuoverne lo sviluppo e favorirne un'armoniosa esistenza nel rispetto delle normative nazionali.

Svolge sia funzioni amministrative proprie sia funzioni delegate dallo Stato, tra le quali, per esempio, i compiti di anagrafe e protezione civile.

L'evoluzione normativa di questi ultimi anni ha portato una decentralizzazione normativa verso gli Enti locali, in modo che essi possano gestire direttamente parte degli interessi e delle normative che riguardano il territorio di loro competenza.

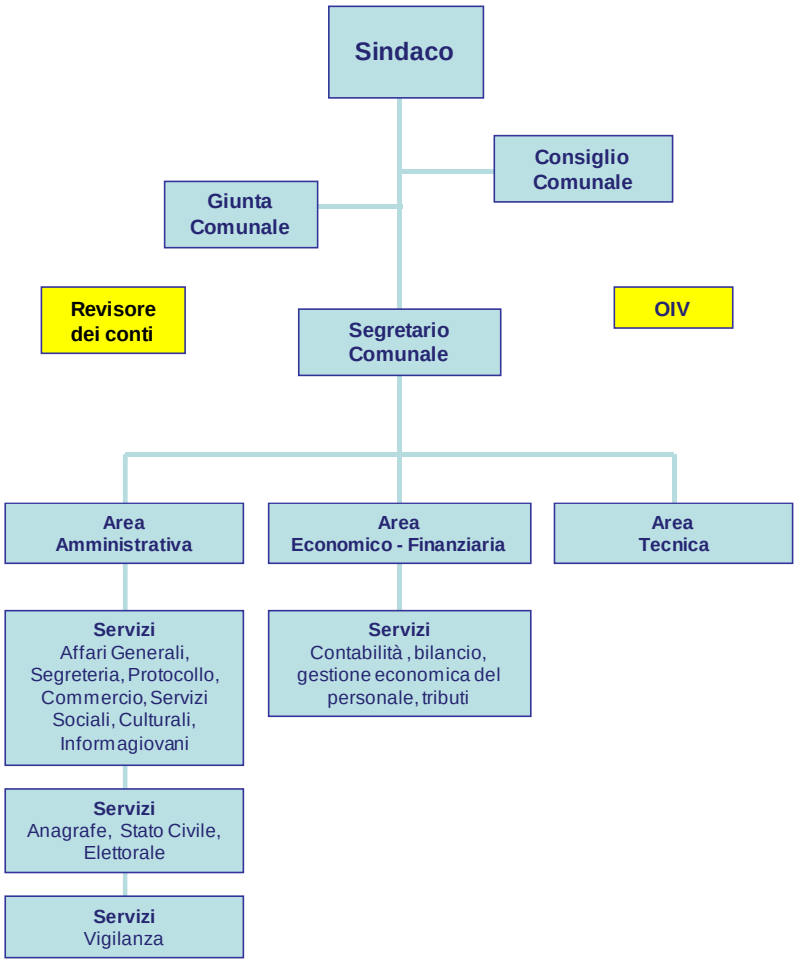
Il **Consiglio Comunale** è l'organo di indirizzo e di controllo politico amministrativo. E' composto dal Sindaco e da n. 6 Consiglieri.

Il **Sindaco**, capo dell'Amministrazione ed Ufficiale di Governo, esercita le competenze stabilite dalla legge. Attualmente riveste la carica di Sindaco la Prof.ssa Filomena Laudato.

Le funzioni della **Giunta Comunale** sono svolte dal Sindaco.

Il **Segretario comunale**, Dott. Nicola Di Rubbo, svolge compiti di collaborazione e funzioni di assistenza giuridico/amministrativa nei confronti degli organi di governo in ordine alla conformità dell'azione amministrativa alle leggi, allo statuto ed ai regolamenti nonché sovrintende allo svolgimento delle funzioni dei dirigenti/responsabili di settore e ne coordina l'attività.

I servizi erogati dal Comune di Arpaise sono quelli rappresentati nella figura seguente, suddivisi nelle unità organizzative già individuate precedentemente.



5 ORGANIGRAMMA DELL'ENTE

Nella tabella seguente è riportata l'organizzazione dell'Ente, con l'indicazione delle Unità Organizzative di Riferimento (UOR), dei rispettivi Responsabili preposti, dei servizi gestiti dalla UOR e dei ruoli rivestiti dal personale.

	Area	Responsabile Area	Incaricati	Compiti assegnati
Segretario Comunale: Dott. Nicola Di Rubbo	Amministrativa	Porcaro Emilio	Donisi Daniela	Affari Generali, Segreteria, Servizi sociali, culturali, informagiovani, protocollo, vigilanza, gestione amministrativa del personale
			Pignatiello Mariangela	Anagrafe, Stato Civile, Elettorale, Servizi sociali
	Economico-Finanziaria	Porcaro Emilio	Marra Orsola	Contablità, bilancio, gestione economica del personale, protocollo, Commercio
	Tecnica	Iuliano Antonio	Iuliano Maria	Tributi
			Domenico Gagliarde	

6 ATTIVITA' DELLE AREE (UOR) E SERVIZI FORNITI

L'amministrazione di Arpaise offre ai cittadini numerosi e importanti servizi fra i quali si evidenziano: polizia locale, nettezza urbana, servizio anagrafe e stato civile, servizi di istruzione e servizi culturali, servizi cimiteriali, impianti sportivi, servizi sociali, illuminazione pubblica, viabilità, servizi tecnici, tutela dell'ambiente, ecc.

Il comune ha una struttura organizzativa articolata in Unità Organizzative di Riferimento, denominate Aree.

Alle Aree sono affidate funzioni ed attività che esercitano con autonomia gestionale, nell'ambito degli indirizzi, degli obiettivi e dei programmi fissati dagli organi politici.

I settori dell'Ente si distinguono in:

- servizi con responsabilità di raggiungimento di obiettivi e risultati attraverso la gestione diretta di risorse umane, strumentali e finanziarie, denominati servizi finali;
- servizi strumentali, con funzioni di supporto ai servizi finali.

Essi sono elencati nella struttura organizzativa rappresentata al paragrafo precedente.

Il sistema di controllo del Comune è articolato in attività di:

- **controllo strategico** finalizzato a supportare le attività di programmazione strategica e di indirizzo politico amministrativo degli organi di governo dell'Ente e ad assicurare la funzione di valutazione dell'adeguatezza delle scelte compiute in sede di attuazione dei piani, dei programmi e degli altri strumenti di determinazione dell'indirizzo politico in termini di congruenza tra i risultati conseguiti e gli obiettivi predefiniti.

- **controllo di gestione**, ovvero il sistema di attività e procedure dirette a verificare lo stato di attuazione degli obiettivi programmati e, attraverso l'analisi delle risorse acquisite e della comparazione tra i costi e la quantità e qualità dei servizi offerti, la funzionalità della organizzazione dell'Ente, l'efficacia, l'efficienza ed il livello di economicità della azione amministrativa allo scopo di ottimizzare, anche mediante tempestivi interventi di correzione, il rapporto tra costi e risultati. Il controllo di gestione è svolto dal Segretario Comunale, anche avvalendosi di specifiche risorse professionali.
- **controllo di regolarità amministrativa e contabile** che deve rispettare, in quanto applicabili alla Pubblica amministrazione, i principi generali della revisione aziendale asseverati dagli ordini e collegi aziendali operanti nel settore. Esso è esercitato per le parti di relativa competenza dalle seguenti figure:
  - Segretario Comunale, per quanto attiene al controllo di regolarità amministrativa e all'attività di consulenza tecnico giuridica;
  - Responsabile del Area Finanziaria e dal revisore dei conti per quanto attiene alla regolarità contabile e alla copertura finanziaria;
  - singoli Responsabili di Area per le specifiche attribuzioni loro conferite.

7 FIGURE RESPONSABILI

Di seguito sono indicate le figure coinvolte nel processo di gestione documentale tra le quali esiste una responsabilità condivisa:

Ruolo	Responsabile	Vicario (In caso di vacanza, assenza o impedimento del Responsabile incaricato)
Responsabile per la gestione documentale (responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi)	Dott.ssa Orsola Marra	Dott.ssa Daniela Donisi
Responsabile per l'informatica, ovvero del Sistema Informativo Comunale	Da individuare	
Responsabile per la protezione dei dati personali, ai sensi del D.Lgs. 196/2003 (codice privacy).	Responsabili delle Unità Organizzative di Riferimento	n.a.
Responsabile del Disaster Recovery e della Continuità Operativa	Da individuare	
Responsabile della conservazione	Da individuare	

8 AMMINISTRATORE DI SISTEMA

In attuazione del punto c) del provvedimento del Garante del 27-11-2008 pubblicato in gazzetta ufficiale n. 300 del 24-12-2008 "Funzioni di amministrazione di sistema",

l'Amministrazione Comunale ha predisposto la Procedura Organizzativa "Amministratori di Sistema" dove sono descritte dettagliatamente le funzioni affidate a questa figura professionale.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Procedura Organizzativa
Uso della Posta Elettronica Certificata e tradizionale

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo documento viene fornita la procedura organizzativa per l'utilizzo della Posta Elettronica Certificata e tradizionale all'interno del Comune di Arpaise.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 SCOPO

Questo documento fornisce la procedura organizzativa sull'utilizzo della Posta Elettronica Certificata, definendo le regole a cui gli operatori devono attenersi nell'utilizzare questo strumento tecnologico, quindi rappresenta una pratica guida operativa nella gestione del processo di protocollazione e trasmissione di documenti digitali attraverso lo strumento di Posta Elettronica Certificata.

1.1 Applicabilità

Il documento è applicabile alla specifica realtà del Comune di Arpaise.

1.2 Aree oggetto d'intervento

Sono interessati tutti i settori e i servizi dell'Ente.

2 RIFERIMENTI NORMATIVI

Il presente regolamento disciplina le modalità di gestione e di utilizzo della Posta Elettronica Certificata nell'ambito del Comune di Arpaise, ai sensi della Legge Bassanini nr. 59/1997, del D. Lgs. 7 marzo 2005, n. 82, del D. Lgs. 30 dicembre 2010, n. 235 e succ. modd. e intt..

3 POSTA ELETTRONICA CERTIFICATA ED AMBITO DI UTILIZZO

La posta elettronica certificata è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna dei documenti informatici al destinatario.

La casella di Posta Elettronica Certificata viene assegnata ad utenti per i soli fini istituzionali ed in considerazione del ruolo e della funzione ricoperti nell'ambito dell'Ente.

La trasmissione dei documenti per Posta Elettronica Certificata:

- disciplina la ricevuta di accettazione e di consegna;
- equivale alla notifica a mezzo posta (raccomandata A/R);
- garantisce autenticazione ed opponibilità ai terzi della data e dell'ora di trasmissione e di ricezione del messaggio;
- consente la gestione dei messaggi imbustati e firmati con la verifica della provenienza e dell'integrità dei messaggi stessi;
- consente la comunicazione dei documenti validi ai fini del procedimento amministrativo;
- permette lo scambio dei documenti informatici ed informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di PEC. Ai sensi dell'art. 4 del D.P.R. n. 68/2005, per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.

La trasmissione del messaggio e la ricezione da parte del destinatario sono certificate dai gestori di posta elettronica certificata (PEC) del mittente e del destinatario, attraverso la

"ricevuta di accettazione" prodotta dal primo e la "ricevuta di avvenuta consegna" prodotta dal secondo.

Il documento informatico trasmesso mediante PEC, affinché soddisfi il requisito legale della forma scritta e possieda valore giuridico-probatorio opponibile ai terzi, deve essere sottoscritto con firma digitale.

Il Comune di Arpaise, ai sensi dell'art. 14 del D.P.R. n. 68/2005, si avvale del servizio di PEC erogato da Gestori di Posta Elettronica Certificata iscritti nell'elenco dei gestori di PEC tenuto dall'ex Centro Nazionale per l'Informatica della Pubblica Amministrazione (CNIPA), ora Agenzia per l'Italia Digitale (AGID), ed i relativi contratti sono stipulati nel rispetto della normativa vigente in materia.

4 SOGGETTI DEL SERVIZIO DI PEC

I soggetti del servizio di posta elettronica certificata, secondo quanto stabilito dalla presente procedura organizzativa, sono:

- il mittente
- il destinatario
- i gestori del servizio di posta elettronica certificata

Nel processo di gestione interna del servizio di PEC dell'Ente agiscono:

- il Comune di Arpaise in quanto proprietario del dominio di Posta Elettronica Certificata e titolare del contratto di fornitura stipulato con il Gestore;
- i Gestori, in conformità con le disposizioni contenute nel DPR 68/2005 e nel D.M. del 2.11.2005;
- l'utente PEC, inteso come il dipendente del Comune di Arpaise o il soggetto che, ricoprendo una carica o svolgendo un compito istituzionale, debba essere assegnatario di una casella di PEC;
- l'incaricato PEC.

4.1 L'incaricato PEC

L'incaricato PEC amministra il dominio di Posta Elettronica Certificata dell'Ente creando, cancellando e gestendo le caselle di posta elettronica certificata ed i relativi utenti, a seguito di formali autorizzazioni.

L'incaricato PEC provvede inoltre a:

- fornire supporto nella redazione/aggiornamento delle presenti istruzioni;
- predisporre ed aggiornare l'elenco delle caselle di PEC e degli utenti PEC autorizzati all'utilizzo del servizio, sulla base delle direttive impartite dal Sindaco;
- supportare gli utenti PEC nell'utilizzo del sistema di PEC;
- monitorare i livelli di servizio erogati dal Gestore.

4.2 Il gestore e i suoi obblighi

I gestori di posta elettronica certificata, che devono essere inclusi in un apposito elenco pubblico gestito e controllato da all'AGID, devono garantire la riservatezza, la sicurezza e l'integrità nel tempo delle informazioni contenute nella cosiddetta "busta di trasporto".

Sono tenuti a trasmettere il messaggio dal mittente al destinatario, integro in tutte le sue parti, includendolo nella busta di trasporto; durante le fasi di trasmissione del messaggio i

gestori mantengono traccia delle operazioni svolte su un apposito "log" dei messaggi per trenta mesi.

Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche ed organizzative che garantiscono la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.

I gestori devono prevedere operazioni di emergenza che in ogni caso assicurino la trasmissione ed il rilascio delle ricevute.

4.3 L'utente PEC e i suoi obblighi

L'utente PEC è tenuto ad attenersi alle disposizioni tecnico-organizzative riportate nel presente regolamento e ad assicurare la diligente custodia delle proprie credenziali di autorizzazione ed il corretto utilizzo della casella di PEC assegnata.

L'utente PEC è responsabile in sede civile, penale ed amministrativa del contenuto dei messaggi inviati e usa la PEC per i soli fini istituzionali.

L'utente PEC deve assicurarsi che i messaggi inviati e ricevuti e le corrispondenti ricevute siano periodicamente salvati su supporti informatici che ne consentano la conservazione nel tempo.

5 ORGANIZZAZIONE DEL SERVIZIO PEC

Tipologie di caselle PEC

Le caselle PEC definite sono distinte in:

- **casella istituzionale:** è quella che identifica l'Ente ed è accessibile solo all'Ufficio protocollo;
- **caselle di struttura**: sono quelle assegnate a strutture dell'Ente. In tal caso, l'utente PEC autorizzato ad accedere alla casella è il responsabile pro tempore della struttura, a meno che quest'ultimo non autorizzi, per iscritto, altro dipendente afferente alla propria struttura;
- **caselle personali**: sono quelle assegnate a un soggetto fisico con provvedimento del Responsabile di Settore. In questo caso, l'utente PEC autorizzato ad accedere alla casella è l'assegnatario della stessa.

Creazione di una casella PEC ed attivazione dell'utente PEC

La creazione di una casella PEC comporta l'attivazione dell'utente PEC le cui credenziali di autenticazione informatica al servizio sono fornite all'assegnatario della casella personale oppure, nel caso di casella istituzionale e di struttura, al responsabile pro tempore della struttura ed, eventualmente, all'incaricato formalmente designato.

Cessazione di una casella PEC e disattivazione dell'utente PEC

La cessazione di una casella PEC comporta la disattivazione dell'utente PEC. La disattivazione dell'utente PEC associato ad una casella di struttura avviene in seguito a cessazione o decadenza dall'incarico del responsabile. La disattivazione dell'utente PEC associato ad una casella personale avviene con provvedimento del Sindaco.

Caselle PEC attivate

All'interno dell'Ente sono state attivate una "casella di PEC istituzionale", assegnata all'Ufficio protocollo:

Nr. 1 casella di PEC istituzionale	comunearpaise@asmepec.it

n. 1 caselle di struttura di cui si riporta l'elenco:

Nr. 1 casella assegnata all'ufficio Anagrafe	anagrafe.arpaise@asmepec.it

5.1 Coordinamento con il protocollo informatico

Il documento informatico ricevuto da un ente o soggetto esterno o spedito dall'Ente ad un altro ente o soggetto esterno, ancorché trasmesso a mezzo PEC, ai sensi dell'art. 53, comma 5, del D.P.R. 445/2000, deve essere protocollato mediante il sistema del protocollo informatico ed includere la segnatura di protocollo secondo quanto previsto dalla normativa suddetta e successive modificazioni.

5.2 Trattamento dei dati personali e segretezza della corrispondenza "PEC"

Il Comune di Arpaise è il titolare, per il perseguimento dei propri fini istituzionali, tra gli altri, del trattamento dei dati personali connesso al servizio di PEC.

Se richiesto dal Gestore, il Comune di Arpaise comunica allo stesso i dati personali degli utenti, secondo il principio di pertinenza, non eccedenza e di necessità rispetto alle finalità perseguite.

Ai sensi dell'art. 49 del D. Lgs. n.82/2005, il Gestore garantisce la segretezza della corrispondenza trasmessa.

6 MODALITA' OPERATIVE PER L'UTILIZZO DELLA PEC

Si rappresentano in questo capitolo le modalità operative per il corretto funzionamento delle caselle di PEC assegnate all'interno del Comune di Arpaise e sopra specificate.

6.1 Utilizzo casella di PEC istituzionale

In questo paragrafo vengono descritte le modalità per la trasmissione di documenti in formato digitale attraverso la casella di PEC istituzionale, integrata al protocollo elettronico.

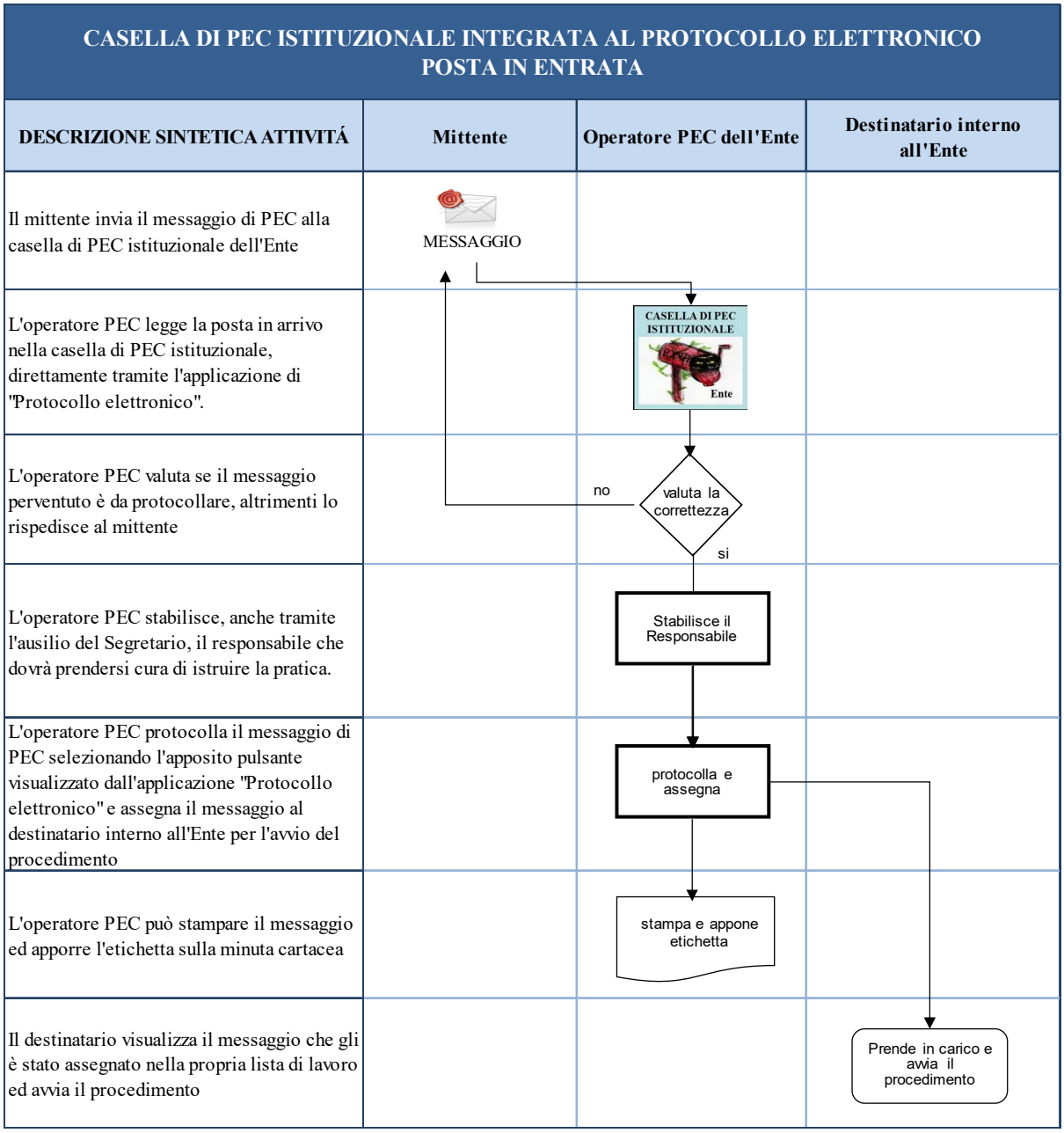
6.1.1 Posta in entrata

La casella viene gestita da un unico operatore/utente autorizzato (in seguito detto "Operatore PEC"), addetto dell'Ufficio "*Protocollo, Gestione documentale e Archivio*", da individuare con specifico atto a cura del Responsabile del Servizio per la Gestione documentale.

L'Operatore PEC riceve la posta nella casella di PEC istituzionale e la consulta direttamente attraverso l'applicazione di "Protocollo Elettronico", selezionando l'apposita funzione di menù.

L'Operatore PEC esamina il messaggio, decide se è da protocollare, seleziona l'apposito pulsante e lo protocolla, quindi lo inoltra al destinatario interno per l'avvio della pratica; se necessario stampa il corpo del messaggio ed appone l'etichetta.

Nella figura seguente viene rappresentato graficamente il flusso appena descritto.

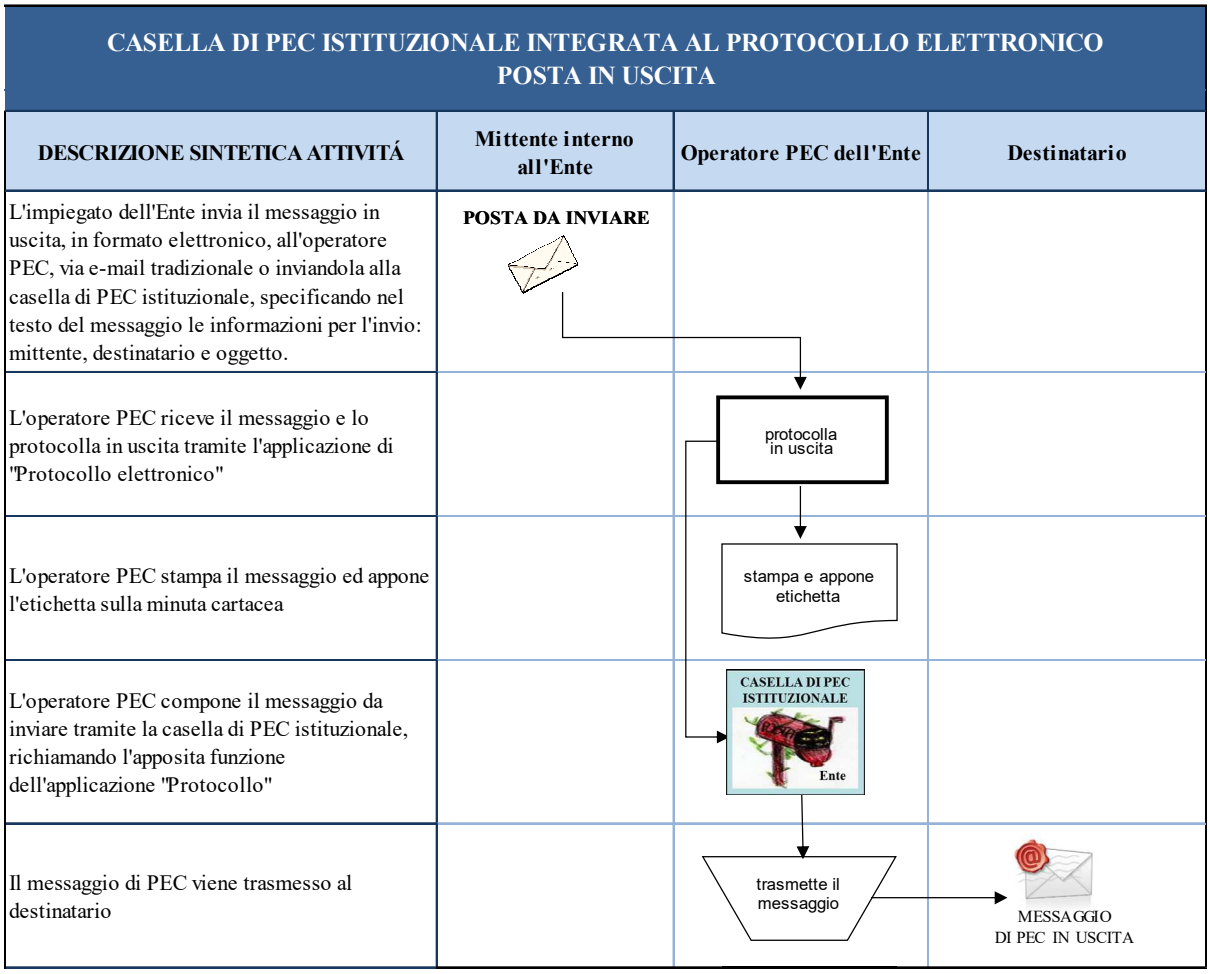


6.1.2 Posta in uscita

La posta da inviare viene fatta pervenire all'Operatore PEC in formato elettronico.

L'operatore PEC protocolla in uscita tramite l'applicazione "*Protocollo elettronico*", effettua una stampa e appone l'etichetta sulla minuta cartacea; quindi, effettua l'invio elettronico richiamando l'apposita funzione di menù che trasmette automaticamente il messaggio attraverso la casella di PEC istituzionale.

Nella figura seguente viene rappresentato graficamente il flusso appena descritto.



6.2 Utilizzo caselle di PEC assegnate ai responsabili

6.2.1 Posta in entrata

Per il protocollo in entrata questo Comune adotta una soluzione basata sul protocollo centralizzato

Il responsabile riceve la posta nella casella di PEC assegnata alla propria struttura e la inoltra all'operatore di protocollo nella casella di PEC istituzionale, specificando nel corpo del messaggio le informazioni minime, necessarie per la protocollazione all'Operatore PEC: *mittente, destinatario e oggetto*.

L'operatore delegato alla gestione della casella di PEC istituzionale prende in carico il messaggio ed attua il procedimento indicato al precedente paragrafo 6.1.1.

6.2.2 Posta in uscita

Per il protocollo in uscita questo Comune adotta una soluzione basata sul protocollo decentrato.

Il responsabile predispone la posta da inviare, la protocolla direttamente ed effettua l'invio elettronico attraverso la propria casella di PEC, inserendo il numero di protocollo nell'oggetto della mail.

In alternativa, il responsabile può spedire il messaggio tramite la casella di PEC istituzionale, nel qual caso la modalità operativa rientra nel caso descritto al paragrafo 6.1.2.

7 CASELLE DI POSTA ELETTRONICA TRADIZIONALE

L'amministrazione ha dotato i propri dipendenti di caselle di posta elettronica tradizionale. La protocollazione dei messaggi che pervengono a queste caselle di e-mail è regolamentata come segue.

Innanzitutto, viene creata la casella di posta elettronica di appoggio, assegnata all'Ufficio Protocollo.

Tale casella viene configurata sull'ambiente di protocollo, allo stesso modo della casella di PEC istituzionale, pertanto tutti i messaggi che pervengono a questa casella vengono visualizzati direttamente dall'Operatore di Protocollo, nella procedura informatica "Protocollo", per essere protocollati.

7.1.1 Posta in entrata

L'assegnatario della casella di posta elettronica tradizionale riceve la posta, la consulta ed invia i messaggi da protocollare alla suddetta casella di posta elettronica di appoggio assegnata all'Ufficio Protocollo, usando l'accortezza di specificare nel corpo del messaggio le informazioni minime necessarie per la protocollazione: mittente, destinatario, oggetto, ecc.

L'operatore di protocollo

1. consulta la lista dei messaggi da protocollare direttamente tramite la procedura "Protocollo elettronico", selezionando la funzione inserimento.
2. seleziona il messaggio da protocollare;
3. lo protocolla e lo inoltra al destinatario interno per l'avvio della pratica;
4. se necessario, stampa il corpo del messaggio ed appone l'etichetta.
5. Il destinatario vede il massaggio entrando nell'ambiente, sulla propria lista di lavoro.

7.1.2 Posta in uscita

L'assegnatario della casella di posta elettronica tradizionale non è abilitato all'invio di posta protocollata attraverso questo mezzo.

Egli predispone la posta da inviare, la protocolla direttamente, quindi effettua l'invio elettronico attraverso la propria casella di PEC, inserendo il numero di protocollo nell'oggetto della mail.

In alternativa, può spedire il messaggio tramite la casella di PEC istituzionale, nel qual caso la modalità operativa rientra nel caso descritto al paragrafo 6.1.2.

8 NORMA FINALE

Per tutto quanto non espressamente previsto dalle presenti istruzioni si applicano le disposizioni vigenti in materia di Posta Elettronica Certificata.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Procedura Organizzativa
Sottoscrizione documenti informatici

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo documento vengono descritte le regole per l'uso della firma elettronica e digitale all'interno dell'Ente ed è fornito l'elenco dei documenti prodotti dall'Ente, soggetti o meno alla sottoscrizione con firma digitale. Vengono, infine, precisati i ruoli che all'interno dell'Ente sono ammessi alla sottoscrizione con firma digitale.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 RIFERIMENTI NORMATIVI

Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, …*", pubblicato in Gazzetta Ufficiale n. 117 del 21 maggio 2013, che sostituisce il precedente DPCM 30 marzo 2009 sulla materia.

Decreto Legislativo 7 marzo 2005, n. 82, e succ. modd. e intt., recante il Codice dell'Amministrazione Digitale.

2 TIPOLOGIE DI FIRMA

2.1 Firma elettronica

Ai sensi dell'art. 1, comma 1, lettera q) del D. Lgs. nr. 82 del 2005, la firma elettronica è un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica".

Essa rappresenta, quindi, la forma più debole di firma in ambito informatico, in quanto non prevede meccanismi di autenticazione del firmatario o di integrità del dato firmato.

All'art. 21, comma 1 del Codice dell'Amministrazione Digitale sopracitato, il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

Sono firme elettroniche riconosciute da questo Comune le seguenti:

- coppia di credenziali costituita da user-id e password,
- Carta d'Identità Elettronica (CIE),
- Carta Nazionale dei Sarvizi (CNS),
- Tessera Sanitaria Elettronica (TSE),
- documento d'identità dei pubblici dipendenti (Mod. ATe),
- identificazione tramite SPID,
- Passaporto elettronico.

Le credenziali di identificazione, user-id e password, utilizzate per accedere al sistema di gestione documentale costituiscono una firma elettronica e devono essere utilizzate esclusivamente dal soggetto cui sono state assegnate; tale tipologia di sottoscrizione è abilitata solo nelle comunicazioni e nelle registrazioni dove è sufficiente l'identificazione informatica del soggetto che le esegue.

Il servizio informatica dell'Ente garantisce per le credenziali di identificazione rilasciate dall'AOO un livello di sicurezza adeguato all'uso che ne viene fatto.

2.2 Firma elettronica avanzata

Ai sensi dell'art. 1, comma 1, lettera q-bis) del D. Lgs. nr. 82 del 2005, la firma elettronica è l'Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

I documenti sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 dek Codice Civile se la soluzione di firma, conformemente a quanto disposto dall'art. 56 del DPCM 22/02/2013 garantisce:

a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
h) la connessione univoca della firma al documento sottoscritto.

L'utilizzo della firma elettronica avanzata è limitato esclusivamente ai rapporti giuridici che intercorrono tra il sottoscrittore ed il soggetto che eroga soluzioni di firma elettronica avanzata.

In completa aderenza con l'art. 61, commi 1 e 2, del DPCM 22/02/2013, le soluzioni di firma elettronica avanzata adottate da questo Ente sono le seguenti:

1. l'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del Codice, effettuato richiedendo la ricevuta completa di avvenuta consegna (art. 1, comma 1, lettera i) del decreto 2/11/2005 recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata».
2. L'utilizzo della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi, del documento d'identità dei pubblici dipendenti (Mod. ATe), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del codice.

I documenti formati utilizzando le suddette modalità, ai sensi dell'art. 65, comma 2, del D.Lgs. 82/2005 sono equivalenti a quelli sottoscritti con firma autografa apposta in presenza del dipendente addetto al procedimento.

2.3 Firma elettronica qualificata

Ai sensi dell'art.1, comma 1, lettera r) del D. Lgs. 82/05, la firma elettronica qualificata è definita come la firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità è certificata da un certificato qualificato.

È inoltre richiesto l'uso del dispositivo di firma sicuro, capace cioè di proteggere efficacemente la segretezza della chiave privata.

Inoltre, la firma stessa deve essere in grado di rilevare qualsiasi alterazione del documento avvenuta dopo l'apposizione della firma stessa.

Qualunque tecnologia che permetta tale identificazione univoca, rientra nel concetto di "firma elettronica qualificata".

La soluzione di firma elettronica qualificata adottata da questo Ente è la firma digitale.

2.4 Firma digitale

La firma digitale è l'equivalente elettronico di una tradizionale firma apposta su documento cartaceo ed esplica la medesima efficacia di quella autografa rendendo i documenti validi e rilevanti a tutti gli effetti di legge.

All'articolo 21, infatti, il D.Lgs. 82/2005 stabilisce, con un rimando all'art. 2702 del Codice Civile, che la firma digitale (o altra firma elettronica qualificata) fa piena prova fino a querela di falso se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta, equiparando così il documento informatico sottoscritto con firma digitale alla scrittura privata sottoscritta con firma autografa (e non, come avveniva in precedenza, alla scrittura privata con firma autenticata).

La firma digitale è associata stabilmente al documento informatico e fornisce informazioni che attestano con certezza l'integrità dei dati oggetto di sottoscrizione, l'autenticità delle informazioni relative al sottoscrittore e la non disconoscibilità.

Essa è il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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.

Elementi di rilievo del sistema "firma digitale" sono rappresentati dal certificato digitale di sottoscrizione, che l'Ente Certificatore rilascia al titolare di un dispositivo di firma, nonché dal servizio di marcatura temporale del documento informatico che consiste nella creazione di una firma digitale da parte di una Terza Parte Fidata, cui è associata data ed ora certa.

3 MODALITÀ OPERATIVE PER L'UTILIZZO DEI KIT DI FIRMA DIGITALE

L'Ente ha acquistato n 4 kit di firma digitale assegnati ai soggetti in elenco: al Sindaco Prof.ssa Filomena Laudato, al responsabile dell'area Tecnica Antonio Iuliano, al Responsabile dell'area Economico Finanziaria Emilio Porcaro e al segretario comunale Nicola di Rubbo.

Le responsabilità e gli obblighi derivanti dall'utilizzo dei dispositivi di firma digitale sono regolamentati dalla succitata normativa in materia e dal Contratto inviato dal gestore, già firmato per accettazione dai titolari dei kit.

Agli assegnatari dei kit di firma digitale sono impartite specifiche istruzione operative, attraverso specifiche attività formative.

4 SOTTOSCRIZIONE DEI DOCUMENTI

Viene riportato di seguito l'elenco dei documenti prodotti dall'Ente, soggetti o meno alla sottoscrizione con firma digitale.

4.1 Documenti da sottoscrivere con firma digitale

A regime tutti i documenti appartenenti alle categorie seguenti dovranno essere sottoscritti con firma digitale.

- Delibere
- Liquidazioni
- Ordinanze
- Richiesta pareri tecnici diversi Uffici

- Richiesta pareri per consigli di partecipazione
- Richiesta pareri per piani particolareggiati
- Richiesta pareri Urbanistica – OO.PP.
- Richiesta emissione ordinanza
- Richiesta licenze per manifestazioni
- Richiesta accertamenti per utenti ERP
- Richiesta accertamenti per buono affitto
- Richiesta accertamenti edilizia privata
- Richiesta sopralluoghi SUA
- Richiesta attivazione procedimento SUA
- Richiesta pareri COSAP
- Autorizzazione consultazione fondi archivistici e riproduzione documenti
- Comunicazione abusi edilizi
- Rilascio pareri PM
- Rilevazione abusi edilizi
- Comunicazioni per accertamenti abusi
- Comunicazioni al SUA
- Richieste verifiche edilizia privata
- Rilascio pareri edilizia privata
- Rilascio pareri OO.PP.
- Variazioni anagrafiche
- Richieste accertamenti
- Variazioni stato civile
- Richieste notifiche elettorali
- Richiesta notifica precetti
- Trasmissione documentazioni SUA
- Richiesta procedure autorizzatorie SUA
- Verifiche varie SUA
- Contratti
- Richiesta attestazione per esenzione TARSU
- Richiesta verifiche agibilità immobili

Questo Ente ha adottato una logica di passaggio graduale alla firma digitale; pertanto, allo stato attuale vengono sottoscritti con firma digitale solo i documenti appartenenti alle seguenti tipologie:

- Contratti
- Fatture
- Registro giornaliero di protocollo

Man mano che sarà estesa l'adozione della firma digitale ad altre tipologie sopraelencate questo documento sarà aggiornato.

4.2 Documenti da sottoscrivere con firma qualificata

L'Ente deve selezionare dalla lista seguente le tipologie di documenti che intende sottoscrivere con firma qualificata.

- Proposta variazioni bilancio e PEG
- Richiesta proposta attivazione tirocinio
- Richiesta ferie - permessi - straordinario

- Ordinativi economali
- Buoni economali
- Comunicazione elenchi agevolazione rette scolastiche
- Richiesta verifica percorsi scuolabus
- Richiesta dati anagrafico-statistici
- Richiesta pareri tecnici convenzioni e piani di sviluppo
- Richiesta sopralluoghi musei
- Richiesta servizio d'ordine festa dei parchi
- Verifiche condizioni sociali utenti
- Rilascio nulla osta obiettori
- Aggiornamento carichi di lavoro
- Comunicazioni per ordinativi incassi
- Richieste rimborsi
- Comunicazioni per pagamenti aree PEEP
- Comunicazioni pagamenti per attività estrattive
- Predisposizione schema contratti di locazione
- Comunicazioni aggiornamento canoni di locazione
- Comunicazioni per pagamenti contributi
- Rilascio pareri utilizzo strade
- Rilascio nulla osta per tasse consortili
- Invio assegnazione numeri civici
- Predisposizione schema convenzioni
- Rilevazione presenze commissione edilizia ed ambiente
- Richiesta stanziamenti capitoli di bilancio
- Richiesta pareri applicazione IVA
- Certificazioni anagrafiche
- Comunicazione mensile incassi diritti
- Richiesta pagamento fornitura C.I.
- Convocazione CEC
- Nota spese contrattuali
- Buoni d'ordine per forniture
- Comunicazione spese postali
- Comunicazioni varie Gabinetto Sindaco
- Predisposizione tabulati liquidazione stipendi ed assimilati
- Predisposizione bilancio di previsione e rendiconto di gestione
- Completamento delibere lavori e atto liquidazione
- Relazioni P.O. sull'attività gestionale
- Comunicazioni d'incasso
- Comunicazioni rettifiche aggiornamenti
- Richiesta versamento spese gestione c.c.p.
- Report informativi controllo gestione
- Proposte stanziamento bilancio di previsione
- Report SAL PEG CDG STAT SG
- Comunicazioni relative al controllo di gestione S.Q.

4.3 Documenti che non necessitano di alcuna firma elettronica

- Report stato avanzamento PEG
- Convocazioni riunioni diversi uffici

- Richiesta di manutenzioni tecnico/informatiche
- Comunicazioni organizzative
- Informative su legge e circolari
- Verifiche economie di bilancio
- Richiesta riutilizzo economie
- Concessione utilizzo sale pubbliche
- Organizzazione e attività ufficio stampa
- Concessione materiale audiovisivo
- Comunicati stampa attività universitarie
- Corrispondenza gruppo tecnico turismo
- Rilascio elaborazioni statistiche
- Invio dati statistici
- Trasmissione bandi di gara con esiti
- Richiesta e trasmissione informazioni uffici diversi
- Disposizioni di servizio P.M.
- Richieste dati anagrafici
- Assegnazione obiettori
- Autorizzazioni vendite alloggi in aree concesse in diritto di superficie
- Comunicazioni relative ad attestazione ISEE
- Richieste varie utenti ERP e non
- Aggiornamento cartografia
- Invio verbale commissione ambiente
- Richiesta scarto atti Archivio comunale
- Invio atti informativi applicazione contratti e normative fiscali
- Richieste verifiche natura spazi ed aree pubbliche
- Trasmissione tabulati presenze mensa
- Invio prospetto materiale di cancelleria–carta
- Elaborazioni statistiche

5 VERIFICA DELLE FIRME

Nel sistema software di protocollo informatico sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

La sequenza delle operazioni previste è la seguente:

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato;
- verifica della firma (o delle firme multiple);
- verifica dell'utilizzo nell'apposizione della firma di un certificato utente emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate all'AgID con periodicità;
- trasformazione del documento in uno dei formati standard previsti dalla normativa vigente in materia e attribuzione della segnatura di protocollo;
- inserimento, nel sistema documentale dell'Ente, sia del documento originale firmato, sia del documento in chiaro;

- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del software di protocollo informatico per accelerare successive attività di verifica di altri documenti ricevuti.

6 NORMA FINALE

Per tutto quanto non espressamente previsto dalle presenti istruzioni si applicano le disposizioni vigenti in materia di firma digitale.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Procedura Organizzativa
Titolario di classificazione

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato è riportato il titolario di classificazione

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 PREMESSA

L'art. 50, comma 4 del T.U. sulla documentazione amministrativa prevede che le pubbliche amministrazioni adottino per il proprio archivio criteri omogenei di classificazione e archiviazione.

L'art. 56 del medesimo DPR ribadisce che le operazioni di classificazione sono, insieme con quelle di registrazione e di segnatura di protocollo, operazioni necessarie e sufficienti per la tenuta del sistema di gestione dei documenti. Il complesso normativo di questi ultimi anni, all'interno del quale si iscrive il citato DPR 445/2000, non costituisce una novità per lo Stato italiano, che vanta una lunga e gloriosa tradizione in materia di regolamentazione dell'attività di gestione archivistica.

Il titolario/piano di classificazione è uno degli strumenti che si utilizzano nella gestione dell'archivio in formazione. La normativa recente ha in sostanza riconfermato la validità metodologica degli strumenti di lavoro tradizionalmente usati nella pratica archivistica; di pari passo la dottrina ha approfondito l'analisi di tali procedure e ha suggerito ulteriori affinamenti in grado di migliorare la prassi e di consentire l'uso delle nuove tecnologie.

Lo spirito del DPR 445/2000 è di indurre le pubbliche amministrazioni a ripensare alla funzione dell'archivio all'interno delle strutture organizzative, riscoprirne la natura di servizio a supporto dell'intera organizzazione, regolamentarne il funzionamento in modo integrato.

Tutto questo comporta per le pubbliche amministrazioni un oneroso lavoro di adeguamento dei sistemi esistenti.

Per agevolare i Comuni in questa fase la Direzione generale per gli archivi del Ministero per i beni e le attività culturali ha costituito il Gruppo nazionale di lavoro.

Oltre al piano di classificazione, che è l'obiettivo primario, il Gruppo di lavoro ha predisposto anche un prontuario per la classificazione, le linee guida per l'organizzazione dei fascicoli e delle serie e il piano di conservazione.

La comprensione del titolario è presupposto indispensabile per il suo uso corretto nell'ambito dell'intero sistema di gestione archivistica, all'interno del quale esso rappresenta solo uno degli strumenti.

2 GLI STRUMENTI PER GESTIRE L'ARCHIVIO CORRENTE

La normativa prevede, in linea con la tradizione archivistica italiana, che l'introduzione di sistemi di gestione informatica degli archivi consentano di effettuare alcune operazioni e di utilizzare determinati strumenti volti a fornire elementi di garanzia e a consentire una gestione archivistica efficiente ed efficace.

L'art. 56 del DPR 445/2000 impone come necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni le operazioni di:

1. **registrazione**
2. **segnatura**
3. **classificazione**

Ricapitolando i concetti già ampiamente espressi nel presente manuale di gestione documentale, **la registrazione a protocollo** dei documenti consente di individuare in modo univoco il singolo documento all'interno dell'archivio e a certificare in modo inoppugnabile la data nella quale esso è entrato a far parte dell'archivio del soggetto produttore, funzione

quest'ultima indispensabile alla luce delle disposizioni legislative sulla durata dei procedimenti amministrativi. Lo strumento che in Italia si usa da circa due secoli per realizzare l'operazione della registrazione è il registro di protocollo, che si configura come atto pubblico di fede privilegiata e va di conseguenza compilato con le avvertenze e le procedure prescritte dalla legge. La registrazione a protocollo, se eseguita secondo i dettami dell'art. 53 del DPR 445/2000, soddisfa le esigenze di attestazione giuridico probatoria.

Con l'aggiunta di altre informazioni (quali, ad esempio, lo smistamento all'Unità Organizzativa Responsabile e l'assegnazione al Responsabile del Procedimento Amministrativo, la classificazione e l'indicazione del fascicolo di appartenenza) la registrazione a protocollo esplica una potente funzione gestionale tesa a organizzare la corretta stratificazione dei documenti e a controllare i flussi documentali.

La segnatura è – come recita l'art. 55 del DPR 445/2000 – l'apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso, cioè di quelle che vengono registrate a protocollo.

La classificazione è operazione logica in base alla quale ciascun documento, che riguarda una singola e specifica questione concreta, viene ricondotto, in base all'oggetto trattato, a grandi raggruppamenti di ordine generale e di carattere astratto, indicati nel titolario o piano di classificazione.

Il DPR 445/2000 ribadisce l'importanza della classificazione e ne impone l'obbligo. La classificazione si avvale del piano di classificazione.

Il piano di classificazione o titolario è il sistema precostituito di partizioni astratte, gerarchicamente ordinate (dal generale al particolare), fissate sulla base dell'analisi delle funzioni dell'Ente, al quale deve ricondursi la molteplicità dei documenti prodotti, per organizzarne la sedimentazione ordinata.

Il titolario si sviluppa su più livelli, denominati dalla dottrina: titolo, classe, sottoclasse, categoria, sottocategoria.

Questa Amministrazione ha scelto, in linea con le più accreditate tendenze dottrinarie e con le indicazioni dell'AGID (ex AIPA/CNIPA/DIGITPA), e del Ministero per i beni archivistici e culturali di articolare il titolario di classificazione solo su due livelli: i titoli e le classi, proprio per la sua semplicità strutturale e per la conseguente facilità di memorizzazione e di uso.

Il gruppo nazionale di lavoro sopra citato ribadisce che l'operazione di classificazione non deve confondersi con quella delle aggregazioni documentali in fascicoli, serie e repertori e neppure con quella dello smistamento dei documenti, che obbedisce alle logiche organizzative di ciascun Comune.

Lo stesso insiste, inoltre, sulla necessità che il presente titolario, in quanto strumento condiviso e supporto per la interoperabilità, deve essere adottato, senza possibilità di adattamenti e personalizzazioni arbitrarie.

Eventuali altri cambiamenti possono essere proposti al Gruppo, che li vaglierà e, se li riterrà opportuni, li introdurrà perché possano essere adottati da tutti.

La definizione del presente piano di classificazione per i Comuni si rifà alla distinzione tra funzione e competenza: la funzione è il compito istituzionale che la legge attribuisce a un determinato ente (nel nostro caso, ai Comuni); la competenza è l'attribuzione di una funzione a un determinato ufficio del medesimo ente. Le funzioni attribuite ai Comuni sono uguali per tutti i Comuni, grandi o piccoli che essi siano (nel senso che tutti i Comuni sono

chiamati ad esercitare le medesime funzioni); mentre all'interno di due diversi Comuni la medesima funzione può essere attribuita a uffici diversi e perfino all'interno dello stesso Comune le competenze possono cambiare radicalmente da un anno all'altro.

Il titolario di classificazione, che serve per suddividere i documenti in base all'oggetto trattato, deve essere determinato nella sua articolazione tramite l'analisi delle funzioni. In tal caso è possibile stabilire un sistema di classificazione dei documenti omogeneo per tutti i Comuni, il che consente la comunicazione e, in ambiente digitale, l'interoperabilità dei sistemi, richiesta dalla legge.

L'adozione del titolario è un atto di organizzazione dell'ente e pertanto va deliberato dalla Giunta comunale, unitamente al manuale di gestione del quale costituisce parte integrante, sotto forma di allegato. Tale provvedimento va comunque preceduto dalla individuazione, ad opera sempre della Giunta comunale, dell'Area Organizzativa Omogenea (AOO), dalla istituzione formale del servizio per la gestione documentale e dell'Ufficio "Protocollo, Gestione documentale e Archivio" e dall'indicazione del responsabile di tale servizio.

Il titolario serve a organizzare i documenti prodotti dalla data in cui viene formalmente adottato dal Comune; non può in nessun caso essere utilizzato come strumento di riordino dell'archivio già prodotto, che deve essere conservato nella sua struttura e organizzazione originaria.

Il titolario qui adottato è stato prodotto dal Gruppo nazionale di lavoro ed è il risultato di un confronto fra persone dalla vasta e consolidata esperienza, che hanno studiato il problema nella sua complessità con un bagaglio variegato di conoscenze, mettendo a frutto l'evoluzione normativa e il dibattito scientifico che di recente si è positivamente incrementato, coinvolgendo non solo teorici dell'archivistica e dell'amministrazione, ma anche archivisti e amministratori comunali.

3 PRESENTAZIONE

Il titolario, predisposto dal Gruppo nazionale di lavoro si presenta articolato in titoli (indicati in numeri romani) e in classi (indicate con numeri arabi), scritti in carattere tondo.

È corredato con note di rinvio alla normativa che attribuisce ai Comuni le funzioni dalle quali si sono ricavati i titoli e le classi e con le spiegazioni essenziali per la comprensione dell'architettura generale del servizio di classificazione e di costituzione dei fascicoli.

All'inizio di ogni titolo c'è una presentazione specifica del medesimo scritta in carattere corsivo.

Nelle linee guida per l'organizzazione dei fascicoli e delle serie il Gruppo indica le tipologie di fascicoli, serie o repertori che si aprono nell'ambito di ciascun titolo e classe. In questa sede vengono elencati in calce ai singoli titoli i "repertori" e le serie riconducibili a quel titolo.

La sequenza dei titoli è determinata dagli orientamenti normativi, in particolare dal D. lgs. 29/93 poi confluito nel D. lgs. 165/2001, che distinguono le funzioni attribuite alle amministrazioni pubbliche, e dalle interpretazioni dottrinarie in campo archivistico.

Il titolo I quindi è relativo alla funzione primaria e costitutiva.

Il titolo II è riferito alle funzioni gestionali.

I titoli III-V riguardano le funzioni strumentali e di supporto.

I rimanenti titoli trattano le funzioni finali, cioè quelle operative all'interno della funzione primaria (i titoli VI-VIII si riferiscono a funzioni conferite, i titoli X-XIII a quelle delegate; il titolo IX costituisce un titolo cerniera, nel quale convivono entrambi i tipi di funzioni) .

Si ribadisce che la lettura del titolario va comunque compiuta tenendo conto del carattere gerarchico dello strumento; il che significa che non si può estrapolare la classe rendendola avulsa dal contesto del titolo in cui è inserita.

4 SCHEMA RIASSUNTIVO DEL TITOLARIO

	Schema riassuntivo del piano di classificazione per l'archivio comunale
I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario ad acta 14. Organi di controllo interni 15. Organi consultivi 16. Consigli circoscrizionali 17. Presidente dei Consigli circoscrizionali 18. Organi esecutivi circoscrizionali 19. Commissioni dei Consigli circoscrizionali 20. Segretari delle circoscrizioni 21. Commissario ad acta delle circoscrizioni Conferenza dei Presidenti di quartiere
III	Risorse umane

	1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo 8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari 14. Formazione e aggiornamento professionale 15. Collaboratori esterni
IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni
V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze
VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio

	10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive 7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale 2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio 3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri
XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi

5 TITOLARIO / PIANO DI CLASSIFICAZIONE

Titolo I. Amministrazione generale

Questo titolo è stato pensato per i documenti prodotti dal Comune nell'esercizio di funzioni di carattere generale e trasversale, che interessano tutti gli uffici in quanto costituiscono strumento per l'attività amministrativa dell'intero apparato comunale.

1. Legislazione e circolari esplicative
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
3. Statuto
4. Regolamenti
5. Stemma, gonfalone, sigillo
6. Archivio generale
7. Sistema informativo
8. Informazioni e relazioni con il pubblico
9. Politica del personale; ordinamento degli uffici e dei servizi
10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale
11. Controlli interni ed esterni
12. Editoria e attività informativo-promozionale interna ed esterna
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
14. Interventi di carattere politico e umanitario; rapporti istituzionali
15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni
16. Area e città metropolitana
17. Associazionismo e partecipazione

Repertori

- Registro di protocollo
- Repertorio dei fascicoli
- Registro dell'Albo pretorio
- Registro delle notifiche
- Ordinanze emanate dal Sindaco: serie con repertorio
- Decreti del Sindaco: serie con repertorio
- Ordinanze emanate dai dirigenti
- Determinazioni dei dirigenti
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Verbali delle adunanze del Consiglio comunale
- Verbali delle adunanze della Giunta comunale
- Verbali degli organi collegiali del Comune
- Contratti e convenzioni
- Albo dell'associazionismo: elenco delle associazioni accreditate

- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)

Nei Comuni che hanno realizzato il decentramento:

- Deliberazioni dei Consigli circoscrizionali (uno per quartiere)
- Deliberazioni degli Esecutivi circoscrizionali (uno per quartiere)
- Verbali delle adunanze dei Consigli circoscrizionali (uno per quartiere)
- Verbali delle adunanze degli Esecutivi circoscrizionali (uno per quartiere)
- Verbali degli organi collegiali delle circoscrizioni (uno per organo e per quartiere)
- Registro dell'Albo della circoscrizione (uno per quartiere)
- Contratti e convenzioni delle circoscrizioni (uno per quartiere)

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

Questo titolo è stato pensato per gli atti concernenti gli organi di governo, gestione, controllo, consulenza e garanzia, non per quelli da essi prodotti. Si ricordi che la classificazione riguarda la materia, non l'autore del documento, non le funzioni, ma il funzionamento dell'organo.

Le classi di questo titolo possono essere adeguate alle reali strutture esistenti nel Comune. In questo caso si è proposto il numero massimo pensabile di classi. Non tutte le classi verranno sempre utilizzate (si pensi, ad esempio, alla classe 13), ma devono comunque essere previste.

Le classi dalla 16 in poi sono dedicate agli organi attivati nei Comuni che hanno realizzato il decentramento: anche in questo caso le denominazioni degli organi dovranno essere adattate a quanto stabilito nei singoli statuti; qui si sono indicati quelli padovani.

1. Sindaco
2. Vice-sindaco
3. Consiglio
4. Presidente del Consiglio
5. Conferenza dei capigruppo e Commissioni del Consiglio
6. Gruppi consiliari
7. Giunta
8. Commissario prefettizio e straordinario
9. Segretario e Vice-segretario
10. Direttore generale e dirigenza
11. Revisori dei conti
12. Difensore civico
13. Commissario ad acta
14. Organi di controllo interni
15. Organi consultivi
16. Consigli circoscrizionali
17. Presidenti dei Consigli circoscrizionali
18. Organi esecutivi circoscrizionali

19. Commissioni dei Consigli circoscrizionali
20. Segretari delle circoscrizioni
21. Commissario ad acta delle circoscrizioni
22. Conferenza dei Presidenti di quartiere

Repertori

- Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive

Titolo III. Risorse umane[43]

Il titolo è dedicato alle funzioni relative alla gestione del personale, sia esso dipendente o esterno (collaboratori a qualsiasi titolo). Nelle classi andranno inseriti i documenti relativi a questioni non riconducibili a singole persone.

Per i documenti relativi a ciascun dipendente viene istruito un fascicolo nominativo.

1. Concorsi, selezioni, colloqui
2. Assunzioni e cessazioni
3. Comandi e distacchi; mobilità
4. Attribuzione di funzioni, ordini di servizio e missioni
5. Inquadramenti e applicazione contratti collettivi di lavoro
6. Retribuzioni e compensi
7. Trattamento fiscale, contributivo e assicurativo
8. Tutela della salute e sicurezza sul luogo di lavoro
9. Dichiarazioni di infermità ed equo indennizzo
10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza
11. Servizi al personale su richiesta
12. Orario di lavoro, presenze e assenze
13. Giudizi, responsabilità e provvedimenti disciplinari
14. Formazione e aggiornamento professionale
15. Collaboratori esterni

Serie

Fascicoli del personale: un fasc. per ogni dipendente o assimilato

Repertori

- Registro infortuni
- Elenco degli incarichi conferiti
- Verbali dei rappresentanti dei lavoratori per la sicurezza

Titolo IV. Risorse finanziarie e patrimoniali[52]

In questo titolo sono state previste le funzioni conferite ai Comuni in materia di disponibilità di risorse finanziarie e di gestione contabile, quelle relative alla titolarità e gestione del patrimonio comunale, di natura sia immobile sia mobile; alla acquisizione e gestione dei beni e servizi strumentali allo svolgimento delle attività e funzioni finali.

Talune attività del titolo sono state indicate adottando la terminologia dell'atto finale.

1. Bilancio preventivo e Piano esecutivo di gestione (PEG)
2. Gestione del bilancio e del PEG (con eventuali variazioni)
3. Gestione delle entrate: accertamento, riscossione, versamento
4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
5. Partecipazioni finanziarie
6. Rendiconto della gestione; adempimenti e verifiche contabili
7. Adempimenti fiscali, contributivi e assicurativi
8. Beni immobili
9. Beni mobili
10. Economato
11. Oggetti smarriti e recuperati
12. Tesoreria
13. Concessionari ed altri incaricati della riscossione delle entrate
14. Pubblicità e pubbliche affissioni

Repertori

- Mandati
- Reversali
- Concessioni di occupazione suolo pubblico
- Concessioni di beni del demanio statale
- Elenco dei fornitori (facoltativo)

V. Affari legali

Si è deciso di prevedere un titolo specifico dedicato agli affari legali, nonostante l'obiezione che quasi sempre essi si inseriscono all'interno di un procedimento, per due motivi: prima di tutto perché la funzione si configura come eccezionale e straordinaria, poi perché talvolta le azioni legali, i pareri e le consulenze interessano materie diverse e possono rivestire carattere generale e/o preliminare a una pluralità di procedimenti concreti. Inoltre, come ha fatto giustamente notare qualcuno, non sempre c'è un fascicolo precedente al contenzioso (ad esempio, citazione del Comune per danni da cattiva manutenzione delle strade); anche quando la controversia sorge nel corso di un procedimento amministrativo o di un rapporto civile, il contenzioso si configura come subprocedimento specialistico; è opportuno che gli atti delle controversie siano conservati unitariamente.

Si precisano in nota le motivazioni in base alle quali è stata esclusa dal titolo la classe "Levata dei protesti" a suo tempo proposta.

Si è constatato che spesso i fascicoli di causa, ad eccezione di quelli di carattere tributario, si formano presso un professionista esterno, cui l'amministrazione ha affidato l'incarico di rappresentarla: in tal caso sarà cura del Comune recuperare, una volta terminata la causa,i documenti, perché rimangano nella memoria dell'ente.

1. Contenzioso
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni
3. Pareri e consulenze

Titolo VI. Pianificazione e gestione del territorio

Il titolo è dedicato a funzioni, tra loro interconnesse, relative alla pianificazione e gestione del territorio: si sono semplificate al massimo le classi per comprendere nella generalità delle denominazioni la varietà di procedimenti censiti.

1. Urbanistica: piano regolatore generale e varianti
2. Urbanistica: strumenti di attuazione del Piano regolatore generale
3. Edilizia privata
4. Edilizia pubblica
5. Opere pubbliche
6. Catasto
7. Viabilità
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
9. Ambiente: autorizzazioni, monitoraggio e controllo
10. Protezione civile ed emergenze

Repertori

- Concessioni edilizie

Titolo VII. Servizi alla persona

Sono state raggruppate in questo titolo le funzioni attribuite ai Comuni in materia di servizi educativi e formativi (classi 1-4), servizi culturali, sportivi e del tempo libero (classi 5-7), dei servizi socio-assistenziali (classi 8-14). La riconduzione ad un unico titolo di tutte queste funzioni, che assorbono una cospicua mole di attività dei Comuni, è motivata dalla constatazione che molti interventi dei Comuni assumono caratteristiche promiscue e possono venire individuati più propriamente a livello di classe che non a livello di titoli.

Attualmente il Comune esercita funzioni molto circoscritte nel settore dell'istruzione, certo più limitate rispetto al passato recente e remoto, quando era responsabile ad esempio della prima alfabetizzazione e della formazione professionale della popolazione. A parte la gestione diretta degli asili-nido e delle scuole materne comunali, che costituiscono una fetta molto consistente della sua

attività, ad esso spettano funzioni di supporto, di consulenza e di fornitura di servizi.

Grandi possibilità di intervento hanno i Comuni nel settore della cultura e dello sport, settore strategico per la promozione della dignità della persona e per lo sviluppo dell'identità collettiva; per l'organizzazione del carteggio relativo è parso sufficiente prevedere solo tre classi: la prima dedicata al funzionamento delle istituzioni che gestiscono l'attività, la seconda e la terza relativa alle iniziative concrete.

Nello stabilire le classi relative alle funzioni attribuite ai Comuni in materia di aiuto e sostegno delle fasce deboli della società, si è lasciata cadere la logica del titolario Astengo, che individuava i destinatari dei servizi e si è scelto di indicare l'area di intervento, a chiunque diretto.

Rispetto all'edizione precedente è stata inserita la classe 15. Politiche per il sociale, che intende comprendere tutte le iniziative "al positivo", cioè tutto quello che un Comune può

programmare per migliorare il benessere sociale della cittadinanza, una volta fronteggiate le emergenze e le difficoltà previste nelle classi precedenti.

1. Diritto allo studio e servizi
2. Asili nido e scuola materna
3. Promozione e sostegno delle istituzioni di istruzione e della loro attività
4. Orientamento professionale; educazione degli adulti; mediazione culturale
5. Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, etc.)
6. Attività ed eventi culturali
7. Attività ed eventi sportivi
8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio
10. Informazione, consulenza ed educazione civica
11. Tutela e curatela di incapaci
12. Assistenza diretta e indiretta, benefici economici
13. Attività ricreativa e di socializzazione
14. Politiche per la casa
15. Politiche per il sociale

Repertori

- Registri scolastici (del professore e della classe) prodotti dalle Scuole civiche (ove presenti)
- Verbali degli organi di gestione degli Istituti culturali

Titolo VIII. Attività economiche

I Comuni svolgono nel settore delle attività economiche funzioni particolari, spesso complementari a quelle esercitate da altri enti, ad esempio le province: talora essi sono chiamati a monitorare e raccogliere dati, talora devono rilasciare autorizzazioni etc. La novità introdotta dalla normativa recente riguarda il cosiddetto sportello unico per le attività produttive che rappresenta un vantaggio per il cittadino perché gli consente di ridurre i tempi burocratici. Poiché gli interventi dei Comuni sulle attività economiche possono essere molto variegati, si è preferito prevedere classi molto

generali in grado di assicurare l'apertura di fascicoli specifici entro ripartizioni logiche serrate.

1. Agricoltura e pesca
2. Artigianato
3. Industria
4. Commercio
5. Fiere e mercati
6. Esercizi turistici e strutture ricettive
7. Promozione e servizi

Serie

Fascicoli individuali di ciascun esercente attività economiche

Repertori

- Repertorio delle autorizzazioni artigiane
- Repertorio delle autorizzazioni commerciali
- Repertorio delle autorizzazioni turistiche

Titolo IX. Polizia locale e sicurezza pubblica

Questo titolo è dedicato alla prevenzione e alla repressione delle violazioni sia per quanto concerne la circolazione stradale sia per quanto concerne la vita dell'individuo nel contesto sociale e amministrativo, tendente ad assicurare sicurezza ai cittadini; comprende inoltre le funzioni, residue rispetto al passato e tutte delegate, connesse con il controllo dell'individuo singolo o associato.

1. Prevenzione ed educazione stradale
2. Polizia stradale
3. Informative
4. Sicurezza e ordine pubblico

Repertori

- Autorizzazioni di pubblica sicurezza
- Verbali degli accertamenti

Titolo X. Tutela della salute[127]

Il titolo non necessita di particolari commenti, stante la chiarezza con cui la normativa definisce le funzioni dei Comuni nel contesto del sistema sanitario nazionale. Merita rilevare come le funzioni attualmente attribuite ai Comuni dopo l'entrata a regime della riforma sanitaria siano estremamente circoscritte rispetto a quanto avveniva in tempi passati.

1. Salute e igiene pubblica
2. Trattamenti Sanitari Obbligatori
3. Farmacie
4. Zooprofilassi veterinaria
5. Randagismo animale e ricoveri

Repertori

- Repertorio delle autorizzazioni sanitarie
- Repertorio delle concessioni di agibilità

Titolo XI. Servizi demografici

Le funzioni dei Comuni in materia demografica rientrano fra quelle delegate dallo Stato e molte sono esercitate dal sindaco in veste di ufficiale di governo. Si è inserita fra quelle riconducibili senza dubbio alcuno ai servizi demografici anche la materia della polizia mortuaria, che nel titolario Astengo compariva connesso – con indubbia contraddizione in terminos – con la categoria IV Sanità ed igiene, perché in sostanza gli adempimenti burocratici complessi e di diversa natura connessi con l'evento sono riconducibili al controllo che il Comune esercita sulla popolazione. La classe 4 prevede anche la gestione

degli spazi e dei servizi cimiteriali indicati con la denominazione complessiva “cimiteri”. Si precisa che la costruzione del cimitero è funzione edilizia (quindi Titolo VI/classe 5), come pure l’edificazione di tombe da parte dei privati (quindi Titolo VI/classe 3).

Riunificare in questa classe le funzioni connesse con la morte ha il medesimo significato di semplificazione amministrativa e archivistica compiuta per l’industria con l’istituzione dello sportello unico per le attività produttive.

1. Stato civile
2. Anagrafe e certificazioni
3. Censimenti
4. Polizia mortuaria e cimiteri

Repertori

- Registro dei nati
- Registro dei morti
- Registro dei matrimoni
- Registro di cittadinanza
- Registro della popolazione
- Registri di seppellimento
- Registri di tumulazione
- Registri di esumazione
- Registri di estumulazione
- Registri di cremazione
- Registri della distribuzione topografica delle tombe con annesse schede onomastiche

Titolo XII. Elezioni e iniziative popolari

Il titolo è stato previsto per il carteggio prodotto nello svolgimento delle funzioni connesse alle elezioni di varia natura e iniziativa e alla gestione delle iniziative popolari.

1. Albi elettorali
2. Liste elettorali
3. Elezioni
4. Referendum
5. Istanze, petizioni e iniziative popolari

Repertori

- Verbali della commissione elettorale comunale
- Verbali dei presidenti di seggio

Titolo XIII. Affari militari[137]

Il titolo è stato previsto per il carteggio prodotto nell’ambito dell’espletamento di pratiche residue relative a funzioni ormai inesistenti per quanto concerne la leva militare obbligatoria. Le classi 2 e 3 devono essere previste, anche se ci si augura che … non vengano mai utilizzate!

1. Leva e servizio civile sostitutivo

2. Ruoli matricolari
3. Caserme, alloggi e servitù militari
4. Requisizioni per utilità militari

Titolo XIV. Oggetti diversi

Pur essendo il piano di classificazione sopra illustrato esaustivo, non poteva mancare, in coda, il titolo dedicato al carteggio non riconducibile ai titoli precedenti e riferentesi a funzioni non attribuite alla data di approvazione del titolario, il quale va usato con la parsimonia mai sufficientemente raccomandata. L'uso arbitrario e ingiustificato di tale titolo compromette gravemente la corretta stratificazione e sedimentazione dell'archivio e denota incapacità di comprendere la natura e il contenuto dei documenti, oltre che mancanza di impegno responsabile nello svolgimento della gestione archivistica.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Procedura Organizzativa
Amministratori di Sistema

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: Nel presente documento vengono descritte le modalità con cui l'Ente gestisce l'amministrazione dei sistemi, in rispondenza al Provvedimento del Garante per la protezione dei dati personali del 27-11-2008, pubblicato sulla G.U. n. 300 del 24-12-2008.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 SCOPO

Per meglio comprendere lo scopo di questa procedura, si riporta qui un estratto delle considerazioni preliminari del Garante per la protezione di dati personali che dà una perfetta definizione di “amministratore di sistema”.

<< Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

... omissis ...

le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.>>

1.1 Applicabilità

Destinatari di questo documento sono gli amministratori di sistema nonché responsabili ed incaricati designati dall’Ente.

1.2 Obiettivo

L'obiettivo di questa procedura è quello di individuare alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito del Comune, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

L’Amministrazione Comunale intende prestare attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, data la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni.

1.3 Oggetto

Amministrazione delle banche dati informatiche e dei sistemi su cui sono installate.

2 NORMATIVA DI RIFERIMENTO

Sulla G.U. n. 300 del 24 dicembre 2008 è stato pubblicato il provvedimento del Garante per la Protezione dei dati personali, emesso il 27-11-2008, riguardante:

"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008".

Con tale provvedimento il Garante per la protezione dei dati personali,

1. Ai sensi dell'art. 154, comma 1, lett. h) del Codice, nel segnalare a tutti i titolari di trattamenti di dati personali effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;

2. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

b. Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati

comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, al più presto e comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

3 MISURE ADOTTATE DAL COMUNE

Nel Comune di Arpaise è operativo il Sistema Informativo Comunale (S.I.C.) basato sulle applicazioni software censite.

3.1 Funzioni richieste all'Amministratore di Sistema

All'amministratore di sistema è stata affidata la gestione tecnica del S.I.C. a servizio dell'Amministrazione Comunale e della cittadinanza, al fine di assicurare qualità ed efficienza dei servizi offerti dall'Ente, attraverso

- la tenuta in esercizio dei sistemi hardware e degli apparati attivi di trasmissione e ricezione dati;
- il monitoraggio e tuning dei sistemi, ovvero, il controllo continuo dei sistemi in esercizio, con una valutazione periodica delle performance, al fine di garantire un servizio efficiente degli applicativi software attivi ed una elevata disponibilità del servizio durante il normale orario di lavoro;
- il back-up e restore dei dati, cioè, le attività di salvataggio e ripristino dei dati relativi alle applicazioni software in esercizio.
- le attività sistemistiche riguardanti la sicurezza delle postazioni di lavoro, la rete, i server e le basi di dati, ai sensi del D. Lgs. 109/03.

Per raggiungere queste finalità il S.I.C. necessita di un presidio costante con attività sistemistiche, di amministrazione dei sistemi (macchine server, applicazioni software, banche dati) e della rete.

a) Gestione dei sistemi informatici

- Controllo costante del sistema informativo con attività sistemistiche e di amministrazione dei sistemi e della rete:
  - ***Tenuta in esercizio***

    Vengono svolte le attività per la tenuta in esercizio dei sistemi hardware e degli apparati attivi di trasmissione e ricezione dati. Per tali sistemi saranno gestite le attività di accensione e spegnimento e quelle di ripristino in caso di guasti o cadute.
  - ***Monitoring e Tuning***

    I sistemi in esercizio sono oggetto di controllo periodico con una valutazione delle performance, ciò al fine di garantire un servizio efficiente degli applicativi software attivi ed una elevata disponibilità del servizio durante il normale orario di lavoro.
  - ***BackUp e Restore dei dati***

    Sono garantite le attività per il salvataggio e ripristino dei dati relativi alle applicazioni software in esercizio. Il tutto in modalità conforme ai dettami emanati dal codice sul trattamento dei dati personali, di cui al D.Lgs. 196/03.
  - ***Assistenza sistemistica sulle postazioni di lavoro***

    Viene fornita assistenza sulle diverse postazioni di lavoro dei dipendenti degli Enti associati, tenendo sotto costante controllo anche tutti gli aspetti di sicurezza dei dati (autenticazione e autorizzazione, sistemi anti-virus e anti-intrusione, organizzazione file system e repository di dati sicuri)
  - ***Assistenza sistemistica sulle reti***

    Viene garantita l'assistenza sistemistica sulla rete locale.

    Vengono, in merito, gestiti i seguenti servizi:

a) il controllo della rete dati dal punto di vista della sicurezza e dell'anti-intrusione.

b) il controllo del traffico dati con la misurazione periodica delle performance al fine di garantire un servizio efficiente e con elevata disponibilità durante il normale l'orario di lavoro.

3.2 Misure e accorgimenti adottati

Per quanto riguarda le misure e gli accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, sono state poste in essere le seguenti azioni:

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di Amministratore di Sistema è avvenuta previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

b. Designazioni individuali

La designazione quale Amministratore di Sistema è individuale e riporta l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, così come descritti nella prima parte di questo paragrafo.

c. Elenco degli Amministratori di Sistema

Gli estremi identificativi dell'Amministratore di Sistema, con l'elenco delle funzioni ad esso attribuite, sono riportati nel presente documento.

E' resa nota o conoscibile l'identità dell' Amministratore di Sistema nell'ambito dell'Amministrazione Comunale, tramite l'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, e tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58).

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare conserva direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

e. Verifica delle attività

L'operato dell'Amministratore di Sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Sono stati adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni operative
Formati elettronici dei documenti

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: Questo allegato descrive i criteri che indirizzano l'Ente nella scelta dei formati da adottare per la formazione, gestione e conservazione dei documenti elettronici.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 SCOPO

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 ha portato all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

Il presente documento ha lo scopo di fornire dei criteri generali per indirizzare l'Ente nella corretta scelta dei formati da adottare per la formazione, gestione e conservazione dei documenti elettronici, in coerenza con le regole tecniche emanate dalla Presidenza del Consiglio dei Ministri il 13/11/2014.

2 OBIETTIVO

Obiettivo del documento è di permettere all'Ente di adottare formati di documenti elettronici tali da garantire la leggibilità e la reperibilità del documento informatico durante il suo ciclo di vita attivo e successivamente nel tempo.

I formati adottati possono essere aggiornati periodicamente sulla base dell'evoluzione tecnologica, pertanto questo documento è sottoposto a revisione periodica.

3 CRITERI DI SCELTA DEI FORMATI PER LA GESTIONE

3.1 Il formato del documento informatico

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 del file: 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 la sequenza 0xffd8 identifica i file immagine di tipo .jpeg.

Una prima sommaria, e non esaustiva, elencazione dei più diffusi formati, secondo il loro specifico utilizzo, può essere la seguente:

- 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, ...)
- Formati email (SMTP/MIME, ...)

Ai fini della formazione, gestione e conservazione, questo Ente ritiene di dover scegliere formati tali da garantire la leggibilità e la reperibilità del documento informatico durante il suo ciclo di vita attivo e successivamente nel tempo.

3.2 Caratteristiche da considerare nella scelta del formato

Come richiesto dalla letteratura e dalla normativa cogente, le principali caratteristiche che devono orientare la scelta da parte dell'Ente sono:

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

3.2.1 Apertura

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.

3.2.2 Sicurezza

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.

3.2.3 Portabilità

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.

3.2.4 Funzionalità

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.

3.2.5 Supporto allo sviluppo

E' 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.).

3.2.6 Diffusione

La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici.

Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

3.2.7 Ulteriori caratteristiche da considerare

Inoltre, nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

4 CRITERI DI SCELTA DEI FORMATI PER LA CONSERVAZIONE

Una particolare attenzione va rivolta alla scelta dei formati in riferimento alla conservazione digitale. L'esperienza insegna, infatti, che molti dei formati che erano particolarmente in auge nel passato sono ormai pressoché scomparsi e chi possiede ancora contenuti digitali codificati secondo quei formati oggi incontra sicuramente serie difficoltà ad accedervi.

E' molto importante stabilire quali sono i criteri oggettivi per la scelta dei formati dei documenti elettronici che assicurino la loro leggibilità a distanza di venti, cinquanta o più anni, quindi avere ben chiari i requisiti che devono essere presi in considerazione nella scelta di un formato compatibile con un processo di conservazione digitale.

L'individuazione dei requisiti desiderabili per i formati elettronici è stata oggetto di un'intensa attività di studio e ricerca da parte di numerosi enti ed organizzazioni nazionali ed internazionali. A tale proposito si citano un interessante testo del Prof. Stefano Pigliapoco (Università di Macerata), "*La memoria digitale delle amministrazioni pubbliche. Requisiti, metodi e sistemi per la produzione, archiviazione e conservazione dei documenti informatici*", pubblicato nel 2005 dall' editore Maggioli ed una dispensa più recente (febbraio 2010) di Stefano Allegrezza, dal titolo "*Requisiti e standard dei formati elettronici per la produzione di documenti informatici*", da cui sono tratti alcuni concetti espressi qui di seguito.

I requisiti dei formati si distinguono in requisiti generali, applicabili a tutte le tipologie di formati, e requisiti specifici, relativi ad una particolare categoria di formati, quali, ad esempio, i documenti di testo, le immagini, i contenuti audio, etc..

I requisiti generali, a loro volta, possono essere:

- **requisiti generali di primo livello**, che vanno presi in considerazione in prima battuta per operare una selezione iniziale
  - **non proprietà**
  - **apertura**
  - **standardizzazione**
  - **trasparenza**
- **requisiti generali di secondo livello**, non meno importanti dei primi, che vanno presi in esame successivamente dopo aver selezionato i formati sulla base dei requisiti di primo livello, tra i quali citiamo robustezza, stabilità, auto-contenimento, auto-documentazione, indipendenza dal dispositivo, assenza di meccanismi tecnici di protezione, assenza di limitazioni sull'utilizzo, accessibilità, non modificabilità, sicurezza, efficienza.

Si riportano di seguito alcuni chiarimenti relativi ai requisiti generali di primo livello, rimandando alle sopra citate pubblicazioni per una trattazione più completa di tutti i requisiti.

4.1 Non proprietà

Un formato si dice proprietario quando è stato creato da una organizzazione privata (ad esempio, una software house), che ne detiene i diritti di proprietà intellettuale; di conseguenza le sue specifiche vengono gestite esclusivamente da tale organizzazione.

Un formato si dice, invece, non proprietario (o libero) quando la gestione delle sue specifiche non è prerogativa di un'organizzazione privata ma è affidata ad una comunità di sviluppatori che cooperano per la gestione condivisa delle stesse, o ad un organismo di standardizzazione.

Ad esempio, sono proprietari (di proprietà Microsoft) i ben noti formati DOC, XLS e PPT (prodotti, rispettivamente, con Microsoft Word, Microsoft Excel e Microsoft PowerPoint), mentre è non proprietario il formato ODF (prodotto con la suite di office automation OpenOffice.org).

Ai fini della conservazione digitale è preferibile utilizzare formati non proprietari in quanto non sono legati all'esistenza di una specifica azienda che ne detiene la proprietà e che potrebbe, in qualsiasi momento, modificarne le specifiche, renderle inaccessibili, o imporre restrizioni sul loro utilizzo.

4.2 Apertura

La definizione di apertura è quella già riportata nel par. 3.2.1.

Il fatto che un formato sia aperto è indipendente dal fatto che sia proprietario o meno.

Ad esempio, il formato DOC della Microsoft (così come l'XLS e il PPT), oltre ad essere proprietario, è stato, per diversi anni, anche chiuso perché le sue specifiche non erano mai state rese note; invece il DOCX è aperto, dal momento che Microsoft ne ha pubblicato fin dall'inizio le specifiche complete

Un altro esempio è il formato PDF che, pur essendo stato per molti anni proprietario, è sempre rimasto aperto in quando le sue specifiche erano liberamente accessibili.

Il requisito dell'apertura è di importanza fondamentale in quanto solo se le specifiche sono note è possibile la realizzazione di software in grado di interpretare correttamente la sequenza di bit che costituisce l'oggetto digitale.

Tuttavia, il requisito dell'apertura non è sufficiente se non è affiancato dal requisito della completa documentazione, ovvero di una descrizione completa ed esaustiva del formato. Un esempio di formato pienamente documentato è il PDF/A, le cui specifiche sono state riconosciute come standard ISO 19005-1:2005.

4.3 Standardizzazione

Un formato è standard quando le sue specifiche sono state definite o approvate da un organismo di standardizzazione ufficiale (quali l'ISO, l'ANSI, l'ECMA, il W3C, etc.) (standard de jure) oppure quando le sue specifiche sono diventate uno standard grazie alla sua ampia diffusione (in questo caso si parla di standard de facto).

I formati che hanno ottenuto un riconoscimento come standard da parte di un organismo di standardizzazione sono meno soggetti ad obsolescenza.

Ai fini della conservazione, è, quindi, importante scegliere formati che siano standard; gli standard de jure sono, inoltre, da preferire agli standard de facto, dal momento che solo il processo ufficiale di standardizzazione garantisce che non vi siano interessi di parte nella definizione delle specifiche di un formato e nella sua implementazione.

Strettamente connesso al requisito della standardizzazione è quello dell'**ampia adozione**, che fa riferimento al grado di utilizzo di un formato. Questo requisito è molto importante in quanto l'ampia adozione costituisce uno dei principali "deterrenti" contro i rischi legati all'obsolescenza tecnologica. È evidente che, se un formato è ampiamente adottato, esso sarà meno soggetto ad essere abbandonato dalle aziende produttrici di software, le quali saranno in grado di sviluppare strumenti più semplici per la creazione, la fruizione, la migrazione e l'emulazione di file codificati secondo quel formato, senza necessità di specifici investimenti da parte delle istituzioni archivistiche[1].

4.4 Trasparenza

L'ultimo requisito generale di primo livello è quello della trasparenza, che tiene conto del grado di semplicità con cui è possibile ottenere la fruizione di un file60. Un formato è trasparente se è possibile la fruizione dei contenuti digitali codificati secondo quel formato utilizzando semplici strumenti di base (ad esempio, mediante un editor di testo61 nel caso dei documenti di tipo testuale). In realtà il requisito della trasparenza non è assoluto, nel senso che non esistono formati elettronici completamente trasparenti, essendo sempre necessaria l'intermediazione di un sistema informatico per la fruizione di un contenuto digitale; tuttavia esistono formati più trasparenti ed altri meno trasparenti.

Per fare un esempio, mettendo a confronto tre formati, il TXT, l'RTF e il DOC, si può senz'altro affermare che:

- il TXT è in assoluto quello più trasparente in quanto permette di inserire il testo sotto forma di caratteri ASCII, ma non prevede alcuna formattazione;
- l'RTF è meno trasparente del TXT, ma più trasparente del DOC, essendo possibile, in linea di principio e con un po' di buona volontà, interpretare senza l'ausilio di un computer anche i tag utilizzati dal formato;
- il formato DOC risulta il meno trasparente tra tutti.

Un altro aspetto da tenere presente è che la compressione può ridurre la trasparenza. Nel caso sia necessario utilizzarla, è opportuno scegliere algoritmi di compressione che siano aperti, non proprietari, ampiamente documentati, non soggetti ad alcuna licenza e possibilmente standard.

Grazie alla loro semplicità, la maggior parte dei programmi riesce ad interpretare facilmente i formati trasparenti, ed è prevedibile che ciò sarà possibile anche in futuro nel caso in cui il formato dovesse diventare obsoleto o dovessero andare smarrite le sue specifiche.

L'importanza del requisito della trasparenza risulta evidente anche dai casi, ormai numerosi, di perdita di dati digitali che si sono verificati nel corso dell'ultimo cinquantennio.

[1] Cfr. il sito della Library of Congress (US) <http://www.digitalpreservation.gov/formats/index.shtml>: «If a format is widely adopted, it is less likely to become obsolete rapidly, and tools for migration and emulation are more likely to emerge from industry without specific investment by archival institutions».
Si veda anche Frequently Asked Questions (FAQs) ISO 19005-1:2005 PDF/A-1, luglio 2006, disponibile sul sito dell'AIIM all'indirizzo <http://www.aiim.org/documents/standards/19005-1_FAQ.pdf>: «Adoption - widespread use may be the best deterrent against preservation risk».

5 TIPOLOGIE DI FORMATO

L'allegato 2 al DPCM 13/11/2014 fornisce una descrizione dei formati che, per le loro caratteristiche, possono essere considerati ai fini della conservazione. L'Ente effettua la propria scelta dei formati da adottare orientandosi sulla base dei requisiti fissati nei capitoli precedenti e delle tipologie di formato indicate nella tabella seguente:

Formato	Caratteristiche
PDF	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. E' stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Nell'attuale versione gestisce varie tipologie di informazioni quali: testo formattato, immagini, grafica vettoriale 2D e 3D, filmati. Un documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A. Sviluppato da Adobe Systems (http://www.adobe.com/) - Estensione .pdf Tipo MIME application/pdf - Formato aperto - Specifiche tecniche Pubbliche
PDF/A	Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali. Tra le caratteristiche di questa tipologia di file abbiamo: - assenza di collegamenti esterni, - assenza di codici eseguibili, quali javascript, ecc., - assenza di contenuti crittografati. Queste caratteristiche rendono il file indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo. Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A. Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
TIFF	Sviluppato da Aldus Corporation in seguito acquistata da Adobe. Estensione .tif - Tipo MIME: image/tiff Formato non aperto - Specifiche tecniche Pubbliche Di questo formato immagine raster vi sono parecchie versioni, alcune delle quali proprietarie, che ai fini della conservazione nel lungo periodo sarebbe bene evitare. Questo è un formato utilizzato per la conversione in digitale di documenti cartacei. Il suo impiego va valutato attentamente in funzione del tipo di documento da conservare in considerazione dei livelli di compressione e relativa perdita dei dati.
JPG	Sviluppato da Joint Photographic Experts Group - Estensioni .jpg, .jpeg Tipo MIME: image/jpeg - Formato aperto - Specifiche tecniche Pubbliche

	Il formato JPEG può comportare una perdita di qualità dell'immagine originale. Anche in questo caso, come nel caso dei TIFF, avendo una grossa diffusione, può essere preso in considerazione, ma il suo impiego, correlato ad un opportuno livello di compressione va valutato attentamente in funzione del tipo di documento da conservare. JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web. Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.
Office Open XML (OOXML)	Sviluppato da Microsoft (http://www.microsoft.com - http://www.microsoft.it) Estensioni principali .docx, .xlsx, .pptx - Formato aperto - Derivato da XML Specifiche tecniche pubblicate da Microsoft dal 2007 Possibile presenza codice maligno Comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database. Open XML è adottato dalla versione 2007 della suite Office di Microsoft. Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML. I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008.
Open Document Format (ODF)	Sviluppato da OASIS (http://www.oasis-open.org/) Oracle America (già Sun Microsystems) (http://www.oracle.com/it/index.html) Estensioni .ods, .odp, .odg, .odb - Formato aperto - Derivato da XML Specifiche tecniche pubblicate da OASIS dal 2005. ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione. Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux. Mac. È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.
XML	Sviluppato da W3C - Estensione .xml - Formato aperto

	Specifiche tecniche pubblicate da W3C (http://www.w3.org/XML/) Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: • SVG usato nella descrizione di immagini vettoriali • XBRL usato nella comunicazione di dati finanziari • ebXML usato nel commercio elettronico • SOAP utilizzato nello scambio dei messaggi tra Web Service
TXT	Oltre a XML, per quanto concerne i formati non binari "in chiaro", è universalmente utilizzato il formato TXT. Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.
Formati messaggi di posta elettronica	Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME. Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui ai precedenti paragrafi.

6 FORMATI ADOTTATI

Nel panorama piuttosto variegato di formati esistenti allo stato attuale, non essendo possibile fare previsioni su quale formato riuscirà ad imporsi come standard de jure e/o de facto, nell'intento di fondare su basi solide il processo di conservazione digitale, questo Ente fa ricadere la propria scelta su formati che soddisfino al massimo grado anzitutto i requisiti generali di primo livello (non proprietà, apertura, standardizzazione e trasparenza) e poi il maggior numero possibile di requisiti generali di secondo livello.

In quest'ottica, quindi, stabilisce quanto segue:

Trattamento	Formati adottati
Formazione e trattamento documenti informatici	PDF, PDF/A, TIFF, JPG, OOXML, ODF, XML, TXT
Archiviazione nel repository documentale (Halley Document Server)	Prima dell'archiviazione, i file vengono convertiti in formato PDF, PDF/A
Firma digitale di documenti informatici	Prima della sottoscrizione, i file vengono convertiti in formato PDF/A o PDF.
Produzione di copie informatiche di documenti informatici	PDF, PDF/A
Acquisizione in formato digitale di documenti analogici, mediante scansione	PDF
Acquisizione dall'esterno di documenti non sottoscritti con firma digitale	Formati indicate per la conservazione, ai sensi dell'allegato 2 del DPCM 13/11/2014: PDF, PDF/A, TIFF, JPG, OOXML, ODF, XML, TXT
Messaggi di posta elettronica	RFC 2822/MIME

Allegati ai messaggi di posta elettronica	Sono ammessi i formati elettronici già stabiliti ai punti precedenti

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni Operative
Documenti esclusi dalla registrazione di protocollo e soggetti a registrazione particolare

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato viene riportato l'elenco dei documenti esclusi dalla registrazione di protocollo e di quelli soggetti a registrazione particolare, ai sensi dell'art. 5, commi j e k del D.P.C.M. 3 dicembre 2013.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 DOCUMENTI NON SOGGETTI ALL'OBBLIGO DI REGISTRAZIONE DI PROTOCOLLO

Sono escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000 e dell'art. 5, comma j, del DPCM 3/12/2013, le tipologie documentarie elencate nei paragrafi 1.1 e 1.2.

Gli elenchi proposti sono stati tratti da "i Quaderni" del CNIPA n. 21 febbraio 2006, Supplemento al n. 9/2006 del periodico "InnovAzione" – Allegato 16.16

1.1 Tipologie di documenti di carattere generale

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare
  (es. fatture, vaglia, assegni) (elenco dettagliato al successivo par. 1.3)

1.2 Elenco delle tipologie di documenti specifici in ambito comunale

- Richieste ferie
- Richieste permessi
- Richieste di rimborso spese e missioni
- Verbali e delibere del Consiglio comunitario;
- Verbali e delibere della Giunta esecutiva;
- Determinazioni
- Le ricevute di ritorno delle raccomandate A.R.
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura
- Gli allegati se accompagnati da lettera di trasmissione, ivi compresi gli elaborati tecnici
- Corsi di aggiornamento
- Certificati di malattia
- Variazione sedi ed anagrafe ditte fornitrici
- Convocazioni ad incontri o riunioni e corsi di formazione interni
- Pubblicità conoscitiva di convegni
- Pubblicità in generale
- Offerte e Listini prezzi
- Solleciti di pagamento (salvo che non costituiscano diffida)

- Comunicazioni da parte di Enti di bandi di concorso, di domande da presentare entro....
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Richieste di copia/visione di atti amministrativi
- Non saranno registrate a protocollo le certificazioni anagrafiche rilasciate direttamente
- al richiedente, le richieste e/o trasmissioni di certificati e tutta la corrispondenza
- dell'anagrafe, stato civile e leva diretta agli uffici comunali
- Richieste di affissione all'albo pretorio e conferma dell'avvenuta pubblicazione
- Comunicazioni di cessione di fabbricato ex L. 191/78
- Assicurazioni di avvenuta notifica

1.3 Documenti soggetti a registrazione particolare

Ai sensi dell'art. 53, comma 5 del D.P.R. 20 dicembre 2000, nr. 445, sono esclusi dalla registrazione di protocollo, tra gli altri, tutti i documenti, elencati nei successivi sottoparagrafi, già soggetti a registrazione particolare da parte dell'amministrazione.

Gli elenchi che seguono sono stati tratti da "i Quaderni" del CNIPA n. 21 febbraio 2006, Supplemento al n. 9/2006 del periodico "InnovAzione" – Allegato 16.17.

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.

Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

1.3.1 Elenco delle tipologie di documenti di carattere generale

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- Corrispondenza legata a vicende di persone o a fatti privati o particolari;
- Le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241; dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

1.3.2 Elenco delle tipologie di documenti specifici in ambito comunale

- **Unità Organizzativa Responsabile - Affari generali ed istituzionali**
  - Atti rogati o autenticati dal segretario comunale (registrazione informatica e cartacea);
  - Contratti e convenzioni (registrazione informatica e cartacea);
  - Verbali delle adunanze del Consiglio comunale (registrazione informatica);

- Verbali delle adunanze della Giunta comunale (registrazione informatica);
- Verbali degli organi collegiali del Comune (registrazione informatica);
- Autorizzazioni commerciali (registrazione cartacea);
- Autorizzazioni artigiane (registrazione cartacea);
- Autorizzazioni turistiche (registrazione cartacea);
- Autorizzazioni di pubblica sicurezza (registrazione cartacea);
- Autorizzazioni di polizia mortuaria (registrazione informatica);
- Autorizzazioni igienico-sanitaria e veterinaria (registrazione cartacea);
- Licenze di pesca (registrazione cartacea);
- Certificati di iscrizione all'anagrafe canina;
- Atti di stato civile (registrazione informatica);
- Pubblicazioni di matrimonio (registrazione informatica);
- Carte d'identità (registrazione informatica);
- Certificati anagrafici;
- Tessere elettorali (registrazione informatica);
- Rapporti incidenti (registrazione informatica);
- Verbali oggetti smarriti;
- Verbali CdS (registrazione informatica);
- Richieste permessi transito ZTL.

- **Unità Organizzativa Responsabile - Affari generali ed istituzionali**
  - Fatture attive (registrazione informatica);
  - Liquidazioni (registrazione informatica);
  - Mandati di pagamento (registrazione informatica);
  - Reversali (registrazione informatica);
  - Dichiarazioni ICI (registrazione informatica).
- **Unità Organizzativa Responsabile - Polizia municipale**
  - Registro verbali di violazione regolamenti e leggi varie;
  - Fatture emesse registri IVA;
  - Autorizzazioni sanitarie registro autorizzazioni sanitarie;
  - Autorizzazioni commerciali registro autorizzazioni commerciali;
  - Autorizzazioni di pubblico esercizio registro autorizzazioni di pubblico;
  - I verbali di violazione del Codice della strada ed i verbali di violazioni amministrative.
- **Unità Organizzativa Responsabile - Affari culturali, educativi e sociali**
  - Dichiarazioni per la certificazione ISEE – Riccometro (registrazione cartacea)
- **Altri documenti**
  - Deliberazioni di Consiglio comunale registro delle deliberazioni del consiglio comunale;
  - Deliberazioni di Giunta comunale registro delle deliberazioni della giunta comunale;
  - Determinazioni dei responsabili dei servizi registro delle determinazioni;
  - Decreti protocollati al protocollo generale;
  - Ordinanze registro delle ordinanze;
  - Contratti in forma pubblica;
  - Repertorio dei contratti;

- Documenti anonimi o non firmati non soggetti ad alcuna registrazione;
- Documenti totalmente illeggibili nel testo non soggetti ad alcuna registrazione;
- Documenti con mittente non riconoscibile non soggetti ad alcuna registrazione;
- Fatture senza lettera di trasmissione registrazione a cura dell'ufficio ragioneria;
- Permessi di costruire registro dei permessi di costruire;
- Verbali di violazione Codice della strada
- Registro dei verbali di violazione Codice della strada;
- Atti pubblicati all'Albo pretorio registro pubblicazioni Albo pretorio;
- Atti depositati nella casa comunale registro deposito atti alla casa comunale;
- Notifiche registro notifiche;
- Verbali di violazione regolamenti comunali e leggi varie (escluso il CdS);
- Le denunce di variazioni ai fini ICI;
- La TARSU;
- L'occupazione di suolo pubblico ed altri tributi ed entrate dell'Amministrazione.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni Operative
Descrizione del prodotto software
di protocollo informatico in uso presso l'Ente

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato viene riportata una descrizione funzionale ed operativa del prodotto software di protocollo informatico in uso presso l'Ente.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 MISSIONE

Attraverso il sistema di protocollo informatico la Società Halley Informatica contribuisce al miglioramento del processo di gestione documentale dell'Ente almeno da due punti di vista:

1. Migliorare l'efficienza interna delle amministrazioni attraverso l'eliminazione dei registri cartacei, la diminuzione degli uffici di protocollo, e la razionalizzazione dei flussi documentali.
2. Migliorare la trasparenza dell'azione amministrativa attraverso degli strumenti che consentano un effettivo esercizio del diritto di accesso allo stato dei procedimenti ed i relativi documenti da parte dei soggetti interessati (cittadini ed imprese).

2 OBIETTIVI

Per adempiere alla missione sopra esposta il sistema di protocollo informatico permette, nel completo rispetto della normativa vigente in materia, di:

1. controllare le pratiche;
2. assolvere gli adempimenti che riguardano il protocollo e l'archivio;
3. gestire i trattamenti di documenti informatici;
4. garantire la trasparenza amministrativa;
5. migliorare l'efficienza interna.

Gli obiettivi di cui stiamo parlando sono sicuramente ambiziosi, la necessità di raggiungerli è sicuramente importante, pertanto gli sforzi protesi da Halley in questa direzione sono stati ingenti pur di mettere a disposizione degli Enti locali un potente strumento, semplice da usare, per favorire il loro cammino nella giusta direzione, senza grossi ostacoli.

3 PRINCIPALI FUNZIONALITA'

La procedura software nasce come integrazione delle procedure di protocollo e procedimenti amministrativi, ma è stata anche arricchita di molte altre funzionalità ed utilità.

In estrema sintesi la procedura realizza:

1. la gestione automatica di posta elettronica e documenti elettronici in genere, compresi i fax;
2. l'interoperabilità dei protocolli;
3. la gestione delle firme digitali in diverse maniere efficaci ed efficienti;
4. la gestione del data base documentale;
5. la gestione del lavoro d'ufficio e controllo dei processi (flussi documentali, work flow management) con metodi estremamente efficienti: procedimenti, carteggi e comunicazioni interne.
6. la trasparenza amministrativa con una completa integrazione con l'Urp;
7. il controllo di gestione delle attività d'ufficio con l'integrazione della dotazione organica, dei prodotti di processo, controllo attività e progetti.

La soluzione Halley è basata su una interfaccia html (web) e funziona:

- attraverso i principali browser esistenti sul mercato;
- con i principali tipi di macchina e di sistema operativo;
- senza bisogno di scaricare moduli software sul sistema dell'utente.

4 I COMPONENTI APPLICATIVI

La procedura è flessibile, in quanto è organizzata in "componenti applicativi" (gruppi di funzioni chiamati in seguito anche "moduli") tra loro integrati, pur essendo ognuno di essi utilizzabile autonomamente.

Quindi non è necessario avviare in esercizio tutti i componenti, ma è importante che la visione delle problematiche sia sufficientemente ampia per permettere successivi passi verso una organizzazione veramente efficiente dell'Ente.

Le possibilità offerte dalla procedura Halley permettono ad ogni Ente di realizzare il proprio progetto organizzativo di gestione documentale.

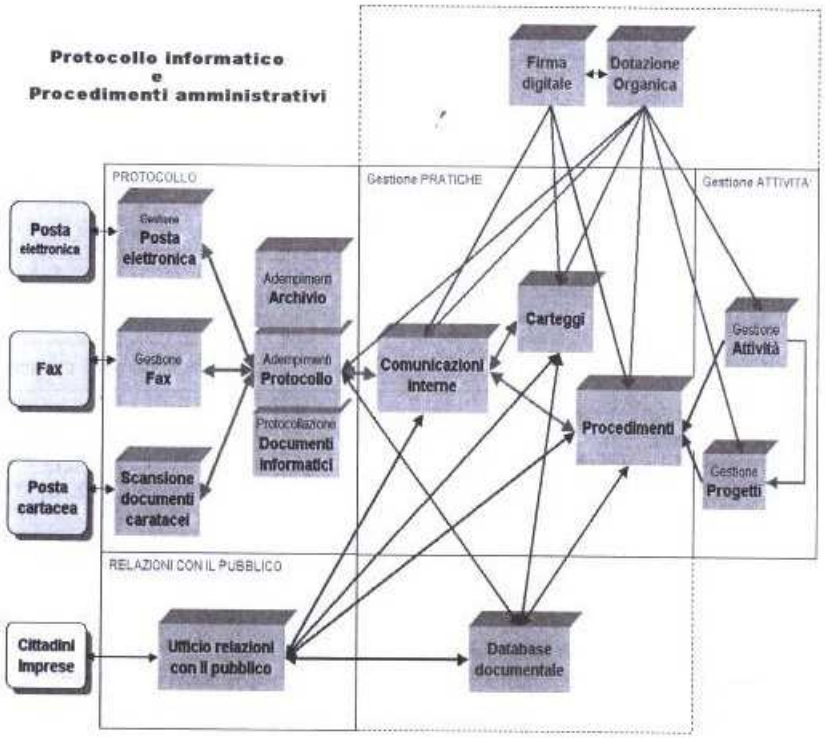
Nella tabella seguente viene fatto un quadro generale dei moduli applicativi correlati agli obiettivi prefissati. Vediamo così come ogni modulo concorre alla realizzazione degli obiettivi stessi.

Nella tabella alcuni moduli sono classificati come "moduli di servizio" perché in realtà non sono utilizzati direttamente dagli operatori, ma sono di supporto ai moduli primari per la realizzazione della logica complessiva della procedura.

Obiettivi	Moduli primari	Moduli di servizio
Controllo pratiche	Procedimenti	
	Atti amministrativi	
	Carteggi	
	Comunicazioni interne	
		Repository documentale (Halley Document Server)
		Dotazione organica
Adempimenti protocollo ed archivio	Adempimenti legge Protocollo	
	Adempimenti legge Archivio	
	Protocollazione documenti informatici	
		Interoperabilità dei protocolli
		Scansione documenti cartacei
Trattamento documenti informatici	Firma digitale	
	Gestione posta elettronica	
	Gestione fax	
Miglioramento efficienza interna	Gestione attività	
	Gestione progetti	
Trasparenza amministrativa	Ufficio relazioni con il pubblico	
	Amminstrazione trasparente	

5 INTEGRAZIONE TRA I MODULI APPLICATIVI

Per una più chiara visione dei vari moduli applicativi, lo schema che segue mostra la loro integrazione.



I moduli sono anche integrati con le altre procedure Halley.

Nelle pagine che seguono viene fatta una breve trattazione dei singoli componenti applicativi.

6 PRESENTAZIONE COMPONENTI APPLICATIVI

6.1 PROCEDIMENTI AMMINISTRATIVI

Finalità

Il componente mira a tenere sotto controllo le 'pratiche' gestite dall'Ente.

Il temine 'pratica' è generico, viene utilizzato semplicemente per indicare un'attività non meglio identificata del lavoro di ufficio.

Mettendo a confronto i termini tecnici con quelli adoperati in ambito amministrativo si parla di:

Processo	**Procedimento**
Flusso del processo (workflow)	Iter dei procedimenti (insieme delle fasi)
Fasi del processo	Fasi del procedimento
Responsabile del processo	Responsabile del procedimento

Il **processo** è una sequenza di fasi finalizzate al raggiungimento di un obiettivo. Ha valore concettuale e teorico. Il termine processo è utilizzato per qualsiasi tipo di attività, ad esempio per un 'processo industriale'.

Il **procedimento amministrativo** è un processo finalizzato all'espletamento di una pratica d'ufficio ed è definito concretamente in termini di tempi, finalità, responsabile, data di apertura, data di chiusura, ecc.

Funzionamento

Quando si rende necessario compiere la prima di una serie di attività finalizzate al raggiungimento di un certo obiettivo, si apre un procedimento.

Il responsabile apre il procedimento inserendo nel relativo database la cosiddetta "testata del procedimento", ovvero informazioni del tipo: data di apertura, motivo, responsabile, tipo di procedimento, richiedente, ecc.

Per ogni altra attività, finalizzata al raggiungimento dello stesso obiettivo, viene aggiunta una fase alla testata del procedimento.

Chi esegue l'attività aggiunge una fase ad un procedimento, inserendo nel database dei procedimenti: data, cosa è stato fatto, da chi, ecc.

Nel momento in cui l'esecuzione di una attività porta al raggiungimento dell'obiettivo prefissato, il responsabile del procedimento chiude il procedimento stesso aggiungendo alla testata del procedimento le informazioni relative allo stato "chiuso", data e provvedimento di chiusura ovvero l'ultima attività eseguita.

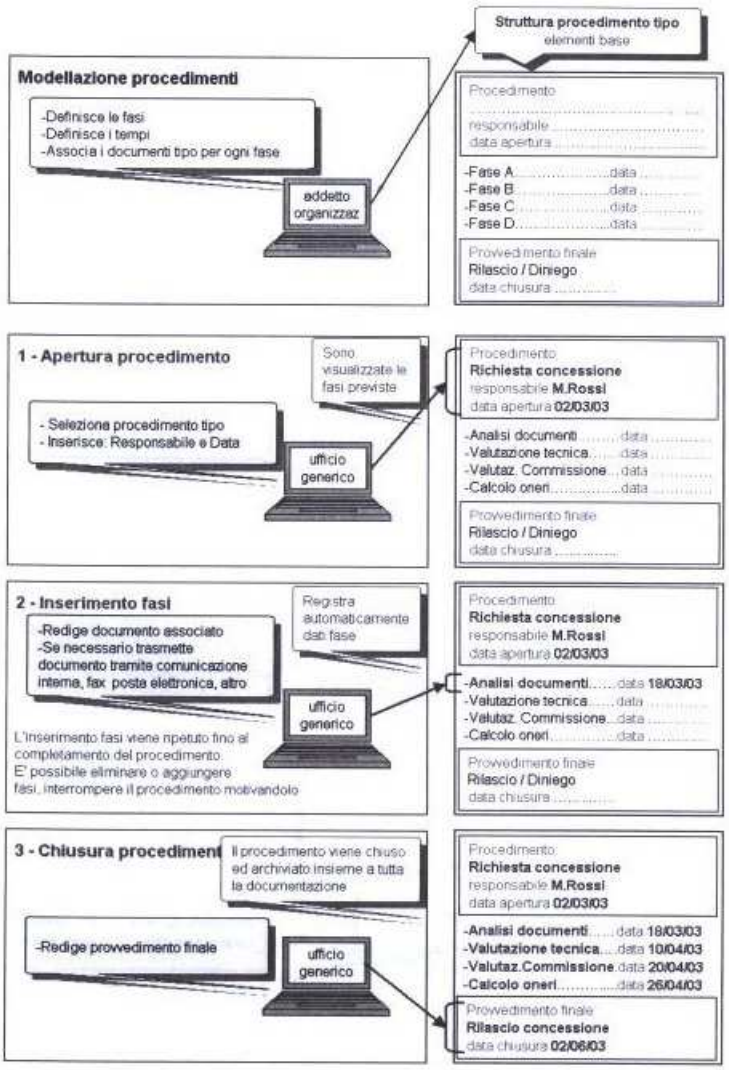
Modellazione dei procedimenti:

Ogni procedimento amministrativo ha un iter predefinito, ovvero una serie di fasi ben codificate. Una parte importante della procedura è la modellazione del procedimento che consiste nel definire:

1. Procedimenti tipo
2. Fasi tipo
3. Campi tipo
4. Testi tipo

Una serie di funzioni complementari permettono di avere il controllo della situazione dei procedimenti, sia aperti che chiusi.

Schema procedimenti



6.2 GESTIONE ATTI AMMINISTRATIVI

Finalità

La procedura consente la gestione delle diverse tipologie di atti amministrativi, quali:

- Delibere di Giunta e Delibere di Consiglio,
- Delibere del Commissario,
- Determinazioni,
- Atti di liquidazione,
- Direttive,
- Ordinanze,
- Decreti,
- Ordini di servizio
- Circolari.

Le utilità messe a disposizione rendono la procedura uno strumento per gestire il lavoro della Pubblica Amministrazione che "parla tramite i propri atti".

La procedura garantisce l'integrità e la conformità degli atti amministrativi e della loro produzione, segue l'iter degli atti amministrativi, permettendo:

- semplicità di inserimento dei dati,
- ottimizzazione del lavoro di gestione, attraverso opportuni automatismi,
- integrità dei dati registrati,
- agevole consultazione.

Costituisce, inoltre, uno strumento di lavoro razionale, al servizio dell'operatore ed offre, agli Amministratori e ai Responsabili dei servizi, un mezzo di controllo immediato e puntuale del lavoro svolto per la produzione degli atti amministrativi.

Funzionamento

Essa si articola nelle seguenti funzionalità:

1. inserimento delle proposte e degli atti definitivi,
2. gestione dei pareri alle proposte,
3. svolgimento dell'iter deliberativo attraverso tutte le sue fasi (istruttoria, ordine del giorno, verbale e deliberazione),
4. gestione degli organi deliberanti,
5. gestione del visto contabile per le determinazioni,
6. stampa personalizzata degli atti,
7. ricerca per numero o per mezzo di uno o più parametri,
8. comunicazione agli uffici delle avvenute deliberazioni,
9. pubblicazione degli atti e relative comunicazioni,
10. comunicazione degli atti esecutivi,
11. controllo situazione proposte e atti definitivi.

La procedura Atti Amministrativi è strutturata, a sua volta, in "Moduli applicativi" (gruppi di funzioni) in modo da rendere il suo utilizzo più flessibile e rispondente alle necessità di ogni Ente.

Si rimanda al manuale utente consegnato all'Ente dalla Società Halley per la presentazione di tutti i moduli applicativi della procedura e per la spiegazione dettagliata delle relative funzionalità.

6.3 CARTEGGI

Finalità

Il componente permette di tenere sotto controllo le 'pratiche' gestite dall'Ente.

Funzionamento

Quando si rende necessario inviare una comunicazione o predisporre un documento che rappresenti la prima di una serie di attività finalizzate al raggiungimento di un certo obiettivo, non avendo a disposizione un procedimento codificato, si apre un carteggio.

Aprire un carteggio significa:

1. farsi carico del raggiungimento dell'obiettivo,

2. dare un nome al carteggio,
3. dare un codice di classificazione,
4. indicare se aperto o chiuso (chi lo apre può chiuderlo),
5. inserire il riferimento ad eventuali soggetti esterni.

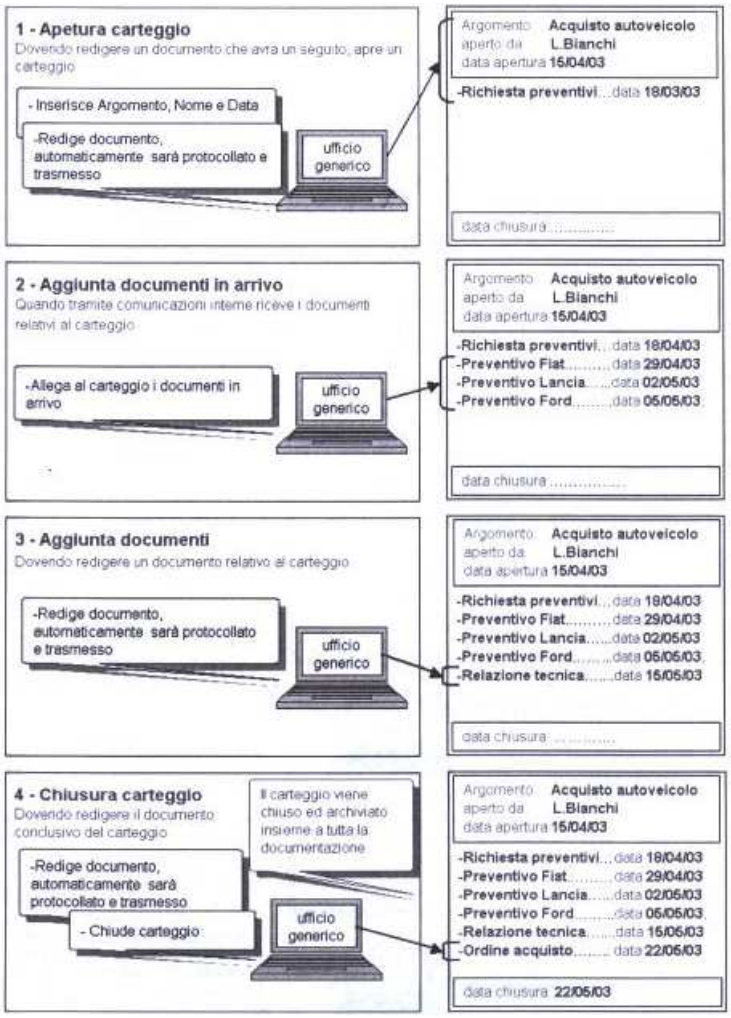
Tutte le attività successive, stesura di altri documenti o invio di comunicazioni verranno fatte aggiungendole in coda al carteggio stesso.

La chiusura di un carteggio consiste semplicemente nel richiamarlo e nell'inserire la data di chiusura.

Utilità collegate sono:

- *situazione carteggi aperti,*
- *stampa elenco carteggi,*
- *stampa registro dei carteggi.*

Schema carteggi



6.4 COMUNICAZIONI INTERNE

Finalità

Il componente permette di tenere sotto controllo le 'pratiche' gestite dall'Ente.

Una funzione molto importante è anche quella della normalizzazione dei documenti prodotti dall'Ente, primo passo essenziale per tutto il progetto di riorganizzazione interna.

I documenti prodotti con la funzione "comunicazioni interne" hanno una immediata collocazione all'interno del sistema informativo ed hanno una struttura normalizzata (estensore, data, oggetto, argomento, tipo di documento informatico), che ne permette una corretta gestione.

Funzionamento

Per l'invio di una comunicazione è sufficiente indicare destinatario ed oggetto della comunicazione, con la possibilità di allegare eventuali documenti.

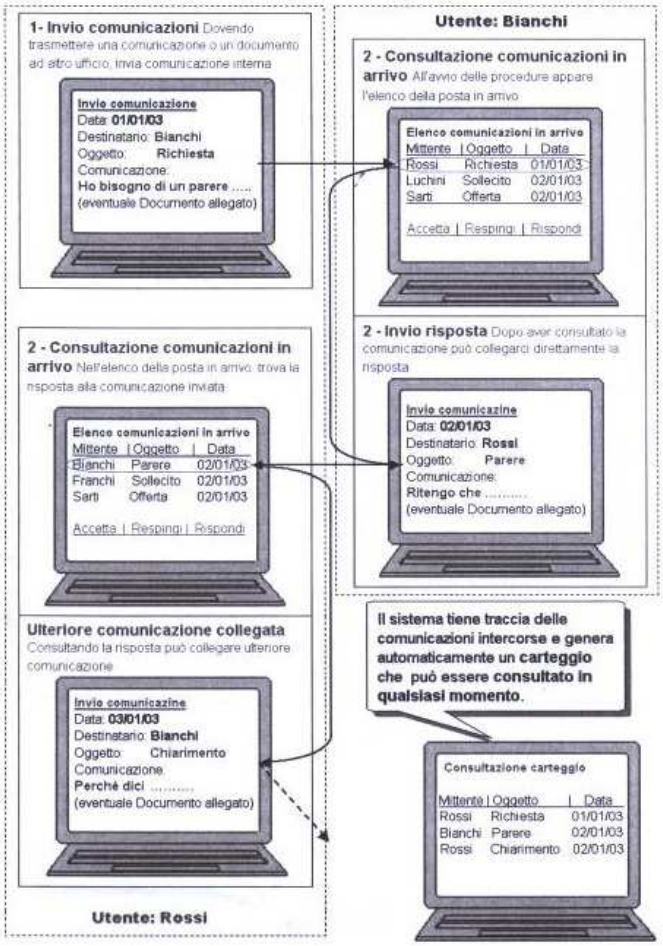
Alla ricezione della comunicazione il destinatario può accettarla respingerla o sub assegnarla. Sempre al momento della ricezione è possibile inviare una immediata risposta che viene automaticamente collegata alla prima comunicazione. In questa fase è anche possibile aprire un carteggio o un procedimento.

Il sistema permette di verificare le comunicazioni non accettate per controllare che vengano tempestivamente vagliate.

Utilità collegate sono:

- *Ricerca e consultazione delle comunicazioni con eventuali documenti allegati, carteggi e procedimenti collegati.*

Schema comunicazioni interne



6.5 REPOSITORY DOCUMENTALE

Finalità

Il componente permette di raccogliere tutti i documenti gestiti da gli altri moduli applicativi, quali, Protocollo, Archivio, Procedimenti, Carteggi, Comunicazioni, Atti amministrativi, archiviarli e, quindi, renderli disponibili per successive ricerche e consultazioni.

Il componente, denominato Halley Document Server, rendendo la gestione e la consultazione dei documenti indipendente dal resto del sistema informativo pur rimanendo completamente integrata ad esso, è progettato specificamente per gestire documenti con la massima efficienza sia in termini di costi che di prestazioni.

Funzionamento

La soluzione applicativa offre le seguenti caratteristiche:

- l'archiviazione dei documenti avviene in maniera automatica dalla procedura in cui si sta lavorando, senza nessun intervento aggiuntivo da parte dell'operatore;
- un potente **motore di ricerca** consente di affinare la ricerca utilizzando diversi criteri, tra i quali:
    - **Ricerca testuale**: permette di trovare i documenti archiviati tramite una qualsiasi parola inserita. Cercando "Mario Rossi" sarà possibile trovare e consultare i mandati, le pratiche edilizie, le determine e qualsiasi altro documento che contiene "Mario Rossi";
    - **Ricerca per operatori logici**: nella ricerca testuale è possibile restringere o estendere il campo di ricerca includendo "and" e "or". Digitando "rossi and verdi" saranno trovati tutti i documenti che contengono sia "rossi" che "verdi";
    - **Ricerca avanzata**: una funzione dedicata permette di rendere più efficace la ricerca utilizzando degli appositi parametri. Così risulta possibile cercare i documenti che contengono "sindaco" nell'oggetto; oppure "inps" nell'anagrafica di riferimento; oppure "malattia" tra i documenti relativi alle risorse umane. Qualsiasi tipo di ricerca può essere inoltre limitata aggiungendo le date di inizio e fine archiviazione;
    - **Ricerca per parole simili**: l'applicativo consente di ricercare per parole simili. Scrivendo "stipendio" trova anche i documenti che contengono "stipendi";
- Ai fini della **consultazione** i documenti sono classificati in due tipologie: documenti pubblici e documenti riservati. I documenti pubblici sono consultabili da tutti, quelli riservati sono consultabili dagli operatori in base al profilo a loro attribuito;
- La gestione e consultazione dei documenti è indipendente dal resto del sistema informativo pur rimanendo completamente integrata. Infatti, anche in caso di modifiche al componente utilizzato, i dati sono conservati e possono comunque essere riletti;
- Il repository documentale è progettato per gestire grosse moli di documenti con la massima efficienza sia in termini di costi che di prestazioni;
- Un sistema di copia automatica si avvia ogni volta che i documenti archiviati occupano la dimensione di un dvd. Per una maggiore sicurezza ogni documento archiviato viene duplicato anche su un altro supporto prima di effettuare la copia definitiva su dvd. Questo sistema garantisce la possibilità di ripristinare il sistema anche in caso di crash.

Tramite il Document Server tutti i documenti sono archiviati separatamente dai normali archivi gestionali. Ne consegue che i dati gestionali, alleggeriti dai documenti (dati non

strutturati), occupano molto meno spazio di memoria e tutte le operazioni ordinarie giornaliere risultano più performanti.

6.6 DOTAZIONE ORGANICA

Finalità

Il componente permette una gestione dei documenti da parte degli operatori dell'Ente che rispecchia l'organizzazione reale, con l'evidente risultato di una gestione complessiva meglio organizzata ed efficiente.

In particolare, ognuno dei soggetti rilasciatari di firme, mittenti e/o destinari di comunicazioni interne e messaggi, addetti al protocollo, responsabili di procedimenti amministrativi, mittenti e/o destinatari di posta elettronica viene collegato univocamente alla dotazione organica dell'Ente.

Il componente permette, altresì, il controllo di gestione delle attività d'ufficio, collegando alla dotazione organica I "prodotti" dei procedimenti amministrativi.

Funzionamento

L'Ente deve gestire la dotazione organica come una funzione dell'ufficio personale. Il collegamento con il protocollo informatico avviene automaticamente perché è la procedura stessa che attinge i dati del personale dagli archivi della procedura "Dotazione organica".

6.7 PROTOCOLLO

Finalità

Il componente permette di gestire l'attività ordinaria dell'ufficio protocollo. Oltre alle funzionalità conosciute, l'applicazione collega tutti i documenti che entrano nell'Ente, siano essi cartacei o elettronici, con le applicazioni di gestione delle pratiche. Facendo l'esempio della posta elettronica (e-mail), queste vengono scaricate dalla casella postale, protocollate se necessario ed Inviate agli uffici competenti come allegati ad una comunicazione interna dalla quale possono iniziare procedimenti e carteggi.

Funzionamento

L'applicazione ha funzionalità molto avanzate, perfezionate e stabilizzate nel tempo, grazie al suo utilizzo quotidiano da parte degli utenti di alcune migliaia di Enti locali che da oltre 15 anni operano con il prodotto di Halley.

Il funzionamento del componente è completamente coerente con quanto descritto nel presente Manuale di gestione documentale. Per una descrizione completa e dettagliata delle funzionalità disponibili e delle modalità d'uso si rimanda al manuale utente consegnato all'Ente.

6.8 ARCHIVIO

Finalità

Il componente permette di gestire l'attività ordinaria dell'ufficio archivio. Le funzionalità offerte, oramai consolidate dall'utilizzo ultradecennale da parte degli utenti, sono di supporto alle attività di classificazione, fascicolazione e archiviazione descritte ampiamente nel presente Manuale di gestione; va però rimarcata l'importanza dell'integrazione delle varie applicazioni, perché senza tale integrazione si crea una abnorme sovrapposizione di funzioni e di attività, a discapito dell'efficienza ed anche dell'efficacia dei lavoro.

I nuovi strumenti di lavoro che la normativa incoraggia ad usare: flussi documentali, work flow management, database documentali, sono nuovi termini, importati dal mondo informatico, per riferirsi a concetti già applicati negli Enti da tempo.

Facciamo alcuni esempi dell'analogia che esiste, in termini di finalità, tra la terminologia usata da sempre e quella divenuta di moda negli ultimi anni:

archivio	database / repository documentale
fascicolo	flusso documentale
procedimento amministrativo	workflow management

La differenza è che per le prime (archivio, fascicoli e procedimenti) esistono delle norme di legge, mentre per le seconde (database documentale, flusso, workflow) ci sono delle 'non meglio definite' linee guida.

In conclusione occorre mettere insieme innovazione-sperimentale e tradizione-consolidata per non rischiare di perdere il vecchio e non ottenere il nuovo, oppure di fare il lavoro due volte. Nel caso specifico, occorre una integrazione tra il modulo " Archivio" che gestisce l'indice dei documenti archiviati ed il "Database documentale'.

Spieghiamo meglio: nell'accezione tradizionale il modulo "Archivio" informatizzava l'indice dei documenti cartacei che venivano fisicamente conservati dentro i "Depositi dell'archivio". Ora accade che i documenti informatici sono fisicamente conservati nel "Database documentale", ma ciò non toglie che debbano essere collegati all'indice dei documenti alla stessa maniera dei documenti cartacei.

Funzionamento

Le funzionalità dell'applicazione si integrano, come gli utenti ben sanno, con quelle del protocollo e servono per produrre i registri di legge.

6.9 PROTOCOLLAZIONE DOCUMENTI INFORMATICI

Finalità

Il modulo nasce per poter trattare i documenti informatici che, non avendo consistenza fisica, creano problemi di identificazione e conservazione. In particolare, mancando la consistenza fisica, manca la possibilità di individuare qualcosa che rappresenti il "Documento originale".

Funzionamento

Il documento informatico appena entra nell'Ente, tipicamente sotto forma di posta elettronica, viene vagliato dal protocollo. Se il documento ha adeguata rilevanza viene protocollato, ne viene calcolata e registrata l'**impronta**[1] e gli viene associata la **segnatura**[2]**.**

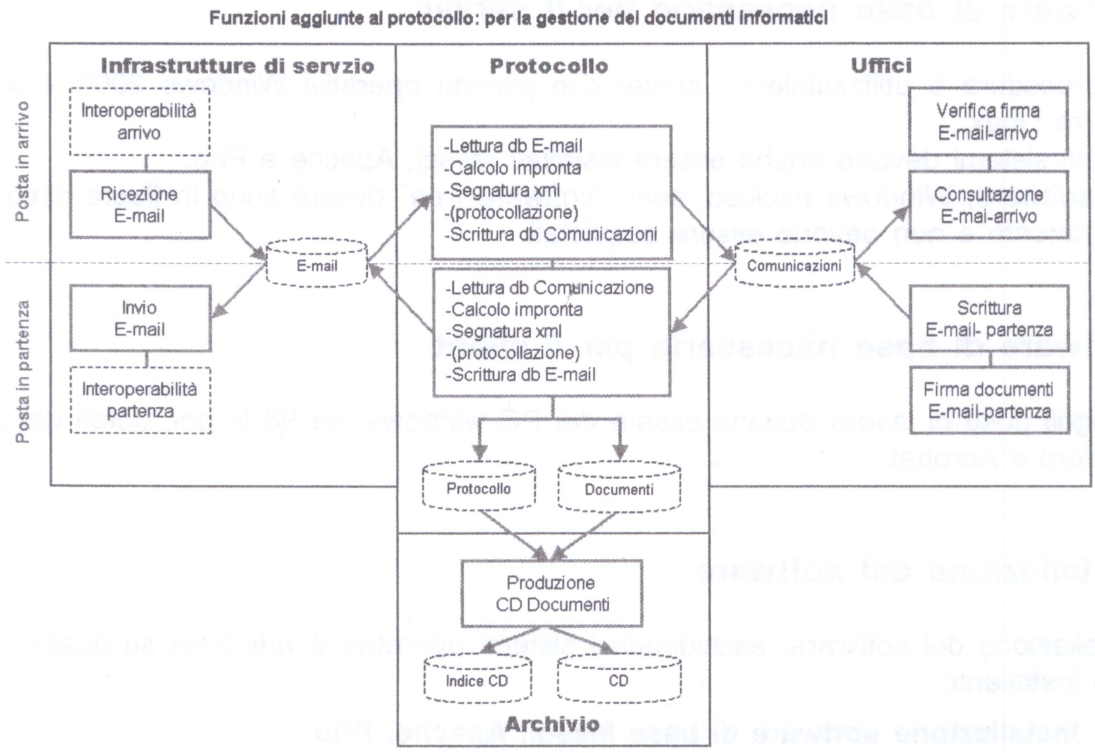
Lo stesso documento, sotto la responsabilità dell'ufficio protocollo, viene archiviato e conservato. Il processo permette di dare al documento una fisicità tale da poterne garantire l'esistenza e la forma originale.

Altro problema collegato alla gestione dei documenti informatici è quello della firma digitale, ma questo non è un problema del protocollo, lo tratteremo a parte. Il protocollo deve garantire il transito dei documenti e l'archivio deve mantenere il documento originale, non è compito di protocollo ed archivio verificare l'autenticità delle firme.

Nella figura seguente viene schematizzato il flusso per la gestione dei documenti informatici.

[1] L'impronta di un documento è una sequenza di 40 caratteri generata da un algoritmo che analizza il contenuto del documento. L'algoritmo garantisce che tale impronta sia di fatto unica per ogni documento, cioè qualsiasi variazione del documento, anche minima, comporta una variazione della sua impronta. Confrontando l'impronta di due documenti, in particolare dell'originale e di una sua eventuale copia, è possibile verificare so I due documenti sono uguali. Il protocollo registra l'impronta del documento per poter poi certificare la corrispondenza esatta,tra documento e protocollo associato.

[2] Per i documenti cartacei la **segnatura** è il timbro che normalmente viene apposto sull'originale con l'indicazione di: nome Ente, data, numero protocollo, ecc, Per I documenti informatici la segnatura consiste nell'allegare gli stessi dati all'originale dei documento informatico in modo che non possano più essere alterati.



6.10 INTEROPERABILITA' TRA PROTOCOLLI

Finalità

Serve per semplificare e rendere più efficiente il lavoro di protocollazione di documenti ricevuti o inviati tramite posta elettronica. I messaggi trasmessi contengono in maniera standardizzata i dati della segnatura in maniera tale che il protocollo che li riceve non deve inserirli manualmente. Inoltre il sistema provvede a restituire al mittente un nuovo messaggio di avvenuta ricezione.

Si tratta di una cooperazione tra mittente e destinatario di messaggio; in pratica per ottenere il vantaggio non basta che sia attrezzato chi riceve il messaggio, ma anche chi lo invia.

Funzionamento

E' una funzione che viene realizzata in maniera automatica dal sistema informatico.

6.11 SCANSIONE DOCUMENTI CARTACEI

Finalità

Il compontente ha lo scopo di migliorare la rintracciabilità dei documenti e ridurre la circolazione del cartaceo, trasformando documenti cartacei in documenti informatici, più facilmente accessibili attraverso il sistema informativo.

La scansione dei documenti, vista da sola, è una operazione semplice che non richiede grandi attrezzature; è, infatti, sufficiente disporre di uno scanner e del software per eseguire la scansione.

E', tuttavia, un'attività onerosa in termini di tempo e di risorse umane da impegnare nell'attività di scansione; inoltre, per far accedere tutto il personale ai documenti scansionati sono necessarie specifiche dotazioni informatiche, sia in termini di hw sia di sw, come PC sufficientemente potenti, rete efficiente, stampanti laser a getto d'inchiostro, componente software per la gestione documentale (HDS).

Inoltre, essa diventa efficace solo se l'Ente è realmente organizzato e se si può ragionevolmente confidare sul fatto che tutti i documenti possano essere trovati nel database documentale.

Il fatto che attraverso il sistema informativo si possa accedere a certi documenti e non ad altri, porta in breve ad un non uso degli strumenti ed alla vanificazione dei vantaggi. Anzi, presto la scansione dei documenti diventa un inutile dispendio di risorse.

La scansione dei documenti è una attività onerosa, pertanto è assolutamente buona norma assumere che:

- i documenti da trattare via scanner siano esclusivamente quelli che arrivano all'Ente dall'esterno in formato cartaceo;
- i documenti prodotti dall'Ente siano redatti esclusivamente, in maniera informatica e normalizzata;
- ove possibile, incoraggiare eventuali Enti esterni a trasmettere i documenti in formato elettronico utilizzando vie telematiche.

E' del tutto irragionevole immaginare che l'Ente abbia l'esigenza di gestire efficacemente i documenti che vengono dall'esterno attraverso la loro scansione e non abbia la necessità di trattare in maniera informatica quelli interni, come è irragionevole pensare che l'Ente produca documenti cartacei per poi trasformarli in informatici.

Funzionamento

L'ufficio protocollo/archivio all'arrivo dei documenti cartacei ne effettua la scansione, li inserisce nel database documentale e, tramite le "Comunicazioni interne", ne invia comunicazione al destinatario che avrà immediato accesso alla copia informatica del documento. Da quel momento tutto l'Ente avrà immediato accesso al documento, accesso comunque controllato dalle abilitazioni fornite ad ogni singolo utente.

6.12 FIRMA DIGITALE

Finalità

Il componente permette di firmare un documento informatico, ovvero di avere certezza di chi ha redatto/approvato un certo documento ed avere certezza che l'immagine del documento che si sta prendendo in considerazione è uguale all'originale.

La procedura utilizza le normali "Firme certificate", ma permette anche di gestire una "Firma digitale interna".

Quest'ultima ha le stesse caratteristiche tecniche di una "Firma certificata", rilasciata da un "ente certificatore autorizzato", ma non ha valore legale nei confronti di terzi essendo rilasciata dall'Ente che la usa. In realtà questo e' un problema relativo perché é sempre una firma della quale l'Ente può certificare o disconoscere la validità anche nei confronti di terzi. Molto di più di un timbro.

L'utilizzo delle "firme digitali interne" non ha alcun costo e semplifica la gestione interna dell'Ente che può decidere in maniera autonoma l'uso da farne e la validità temporale. Lo scopo finale è quello di concentrare in un unico strumento, una smart card di "firma interna" qualcosa che possa assolvere a più esigenze: smart card marcatempo, password accesso procedura e firma dei documenti.

Funzionamento

Firmare un documento è una cosa molto semplice. E' sufficiente individuare il documento, richiamandolo con l'apposito software ed inserire la propria chiave di firma.

Il rilascio di una "firma interna" viene effettuato da un funzionario preposto. Consiste nella consegna fisica della "chiave di firma", prodotta da una apposita funzione del sistema Informatico, ad ogni addetto dell'Ente che ne debba fare uso.

6.13 GESTIONE POSTA ELETTRONICA

Finalità

Il componente permette di attuare una corretta gestione della posta elettronica mantenendo una traccia certa di tutta le e-mail inviate e ricevute dall'Ente. L'applicazione serve per garantire che questo flusso di Informazioni venga trattato come è previsto dalla legge e secondo le regole di gestione interna dei documenti. L'invio e la ricezione di e-mail su caselle non autorizzate, talvolta neanche conosciute dai responsabili dell'ente, eseguito dal personale senza alcun tipo di controllo non fornisce alcuna garanzia sulla qualità e sulle modalità d'uso delle Informazioni trasmesse.

Funzionamento

Le caselle di posta elettronica dell'Ente, usando le password messe a disposizione dai fornitori di servizi e-mail, devono essere rese accessibili solo al responsabile della gestione della posta elettronica, di norma l'ufficio protocollo.

Ricezione dei messaggi: il responsabile provvede alla ricezione dei messaggi che l'applicazione memorizza immediatamente nel suo database prima di trasmetterle ai destinatari finali.

Invio dei messaggi: i messaggi in partenza, prima di essere inoltrati su internet, vengono registrati sul database della procedura.

Controllo del traffico: varie opzioni sono disponibili sul controllo del flusso delle e-mail, ma in generale ci sono due momenti nei quali si può decidere quali protocollare o quali addirittura distruggere: uno, per quelle in arrivo, prima che vengano inoltrate agli uffici; l'altro, per quelle in partenza, prima che vengano inoltrate su internet.

6.14 GESTIONE FAX

Finalità

Il componente è nato per l'invio automatico di fax dal posto di lavoro, per la trasmissione dei fax agli interessati, senza la necessità di stamparli. I fax trattati vengono caricati automaticamente nel database documentale.

Più in generale, essendo il fax un documento elettronico, la procedura evita di trasformarlo in un documento cartaceo per doverlo poi magari anche scannerizzare.

L'invio e la ricezione dei fax vengono intercettati dal servizio di protocollo, per eseguire una protocollazione più veloce, quando necessario.

Funzionamento

I fax in arrivo vengono allegati ad una comunicazione interna ed arrivano così sulla scrivania del destinatario.

Per inviare invece un documento via fax, occorre allegarlo ad una comunicazione interna specificando destinatario e numero del fax.

6.15 GESTIONE ATTIVITA'

Finalità

Il modulo permette lo studio ed il controllo delle attività svolte dall'Ente. Il punto di partenza di qualsiasi progetto organizzativo, perché permette una analisi delle attività svolte per realizzare un obiettivo, "prodotto" in senso ampio. L'analisi dei tempi e delle funzioni impegnate è fondamentale per una azione di BPR (riorganizzazione dei processi).

Funzionamento

Tutte le risorse umane dell'Ente registrano in maniera semplice e veloce le attività svolte durante l'orario di lavoro.

6.16 GESTIONE PROGETTI

Finalità

Dà la possibilità di tenere sotto controllo quelle attività che non rientrano in un processo codificato ovvero ripetitivo. Permette di verificare lo stato di avanzamento di un progetto e di contabilizzare, alla sua chiusura, le risorse impegnate.

Funzionamento

Vengono prima inseriti i progetti ed assegnati ad un responsabile, poi il sistema informatico, in maniera automatica, collega ad ogni progetto le attività che sono state necessarie per realizzarlo. Sempre in automatico, il sistema informatico produce i report di valutazione.

6.17 UFFICIO RELAZIONI CON IL PUBBLICO - URP

Finalità

E' una procedura per l'informatizzazione dell'Ufficio Relazioni con il Pubblico.

Permette al servizio di accedere alle informazioni relative ai procedimenti amministrativi ed a quelle contenute nel data base dei documenti.

Fornisce anche un collegamento diretto con le funzioni di comunicazione interna per

- trasmettere le richieste dei cittadini ad uffici competenti ed Amministratori
- ricevere le risposte
- fornire le risposte ai cittadini.

Funzionamento

Inserisce in un database tutti gli accessi dei cittadini all'ufficio URP.

L'addetto allo sportello, per fornire le risposte, può accedere a:

- data base delle informazioni ricorrenti
- carteggi
- procedimenti
- protocollo
- tributi
- contravvenzioni
- concessioni edilizie
- servizi scolastici
- pagamenti finanziaria
- delibere
- anagrafe

Lo stesso, se non trova una risposta al quesito attraverso le consultazioni di cui sopra, può, a sua volta, inoltrare un quesito a chi di competenza tramite le "comunicazioni interne".

La procedura tiene traccia dei quesiti aperti e produce dei rapporti ad uso dell'Amministrazione e per la valutazione della soddisfazione degli utenti.

6.18 FUNZIONI DI UTILITA' GENERALE

Sono disponibili anche una serie di funzioni di consultazione che permettono, in qualsiasi momento e dal proprio posto di lavoro, di avere informazioni su tutto il lavoro svolto.

Tali informazioni sono sempre utili, spesso indispensabili, per svolgere in maniera efficiente le più disparate attività.

Apposite abilitazioni e password, per ogni tipo di consultazione, permettono di dare accesso solo alle informazioni delle quali ogni profilo professionale (ruolo) ha veramente necessità in relazione alla funzione svolta.

Tra queste si possono citare le seguenti:

- Consultazione comunicazioni
- Consultazione carteggi
- Consultazione procedimenti
- Consultazione documenti
- Consultazione protocollo
- Consultazione archivio
- Consultazione progetti
- Consultazione lavori giornalieri
- Consultazione e-mail
- Consultazione fax

7 USO DELLA PROCEDURA E CORSI DI FORMAZIONE

Imparare ad usare la procedura dal punto di vista operativo è molto semplice non sono necessari corsi appositi, insieme al pacchetto sono forniti tutti gli strumenti per poterla utilizzare.

8 INTERFACCIA UTENTE UNIFICATA

L'uso dei programmi è estremamente semplice perché tutti utilizzano una medesima logica di interfaccia verso l'utente. Dopo aver eseguito anche poche operazioni, l'utente è in grado di muoversi agevolmente tra le varie funzioni della procedura.

Tutti i programmi, per un acceso rapido alle funzioni, utilizzano una simbologia basata su icone standard.

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale

(art. 5 DPCM 3/12/2013)

Istruzioni Operative

Abilitazione all'utilizzo del sistema di gestione informatica dei documenti

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato vengono specificate le abilitazioni allo svolgimento delle operazioni di gestione dei documenti sul sistema informatico.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 ABILITAZIONI ALL'UTILIZZO DELLE FUNZIONALITA' DEL PROTOCOLLO INFORMATICO

Per ogni gruppo di utenti del sistema di protocollazione e gestione informatica dei documenti vengono illustrati i permessi attraverso cui definire le abilitazioni allo svolgimento delle operazioni di gestione del protocollo e dei documenti.

1.1 PROFILI PROFESSIONALI ABILITATI (RUOLI)

Il Sistema informatico di protocollo e gestione documentale può essere utilizzato da utenti appartenenti ai ruoli/profili professionali seguenti:

1. Addetto al protocollo
2. Addetto ufficio generico
3. Responsabile UOR

1.2 MAPPA DEI RUOLI E DELLE FUNZIONI APPLICATIVE

In questo paragrafo vengono dettagliate le attività informatizzate che la procedura prevede per ogni ruolo/profilo professionale.

In particolare, nelle colonne "Attività informatizzate" sono elencate le funzioni eseguite dalla procedura.

1.2.1 Addetto al protocollo

E' la figura che normalmente assolve alle funzioni dell'ufficio protocollo ed archivio (nel seguito trascureremo il dettaglio delle attività che già svolge con la procedura tradizionale).

Con l'introduzione dei documenti informatici, oltre a protocollare ed archiviare i documenti informatici, rappresenta la figura idonea per gestire l'invio e la ricezione di e-mail e fax.

Ruolo	Missione	Attività informatizzate
Addetto al protocollo	Assolvere agli adempimenti di legge ed agevolare la gestione delle pratiche	Protocolla documenti cartacei
		Protocolla documenti elettronici
		Smista i documenti agli uffici
		Stampa adempimenti di legge Protocollo
		Stampa adempimenti di legge Archivio
		Genera CD documenti elettronici e cartacei scannerizzati
		Effettua la scansione dei documenti cartacei
		Riceve e-mail
		Invia e-mail
		Riceve fax
		Invia fax

1.2.2 Addetto ufficio generico

E' la figura che normalmente gestisce pratiche nei vari uffici, praticamente tutto il personale di ufficio dell'Ente.

Ruolo	Missione	Attività informatizzate
Addetto Ufficio generico	Gestire pratiche in maniera efficace ed efficiente	Gestisce comunicazioni e documenti in arrivo
		Controlla validità firme documenti ricevuti
		Redige documenti
		Firma documenti
		Invia comunicazioni
		Gestisce carteggi
		Gestisce procedimenti
		Gestisce progetti
		Inserisce lavori

1.2.3 Responsabile Unità Organizzativa di Riferimento (UOR)

E' la figura che si occupa del controllo delle attività e della gestione.

La procedura mette a disposizione un'ampia gamma di strumenti per analizzare il lavoro svolto dal personale, ma tali dati devono essere studiati ed utilizzati per disegnare una organizzazione coerente ed efficace.

In particolare gli strumenti aiutano a gestire le tre fasi fondamentali del suo lavoro:

- analisi delle attività
- modellazione dei processi
- misurazione dei risultati

La missione del responsabile è quella di controllare le attività svolte per introdurre miglioramenti organizzativi e prevenire problemi di cattiva gestione.

Ruolo	Missione	Attività informatizzate
Responsabile UOR	Avere sotto controllo le attività svolte per introdurre miglioramenti organizzativi e prevenire problemi di cattiva gestione	Controlla accettazione messaggi
		Controlla inserimento lavori giornalieri
		Genera report comunicazioni
		Genera report carteggi
		Genera report procedimenti
		Genera report accessi ufficio relazioni con il pubblico
		Genera report lavori giornalieri
		Genera report progetti
		Modella i procedimenti
		Gestisce dotazione organica
		Inserisce ed assegna progetti strategici
		Gestisce indice firme digitali interne e certificate
		Termina validità firma
		Gestisce caselle postali
		Gestisce apparati fax

1.3 MAPPA DELLE ABILITAZIONI

Funzionalità	Responsabile gestione documentale	Addetto al protocollo	Addetto Ufficio generico	Responsabile UOR
Definizione/controllo abilitazioni accessi	SI	NO	NO	NO
Protocollazione documenti in arrivo	SI	SI	NO	NO
Protocollazione documenti in partenza	SI	SI	SI	SI
Protocollazione documenti interni	SI	SI	SI	SI
Classificazione documenti	SI	SI	SI	SI
Assegnazione ai Responsabili	SI	SI	NO	NO
Fascicolazione documenti	SI	SI	SI	SI
Protocollazione nel registro di emergenza	SI	SI	NO	NO
Consultazione documenti protocollati	SI	SI	Si salvo documenti riservati	Si salvo documenti riservati
Aggiornamento anagrafica mittente/destinatario	SI	SI	NO	NO

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni Operative – Repertori generali

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: In questo allegato è riportato l'elenco dei repertori generali presenti nell'Amministrazione comunale.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-10-2015	Maria Pia Papa	Prima stesura

INDICE

1 Repertori di documenti in doppio esemplare

- Ordinanze emanate da Sindaco
- Decreti del Sindaco
- Ordinanze emanate dai dirigenti (unico repertorio)
- Determinazioni dei dirigenti
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa
- Circolari

2 Repertori di documenti in esemplare unico

- Verbali delle adunanze del Consiglio comunale
- Verbali delle adunanze della Giunta comunale
- Verbali degli organi collegiali del Comune
- Contratti e Convenzioni

Comune di Arpaise
Provincia di Benevento

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Istruzioni operative
Politiche di Sicurezza

Cod. **MANGEDOC** Rev. **1.0** Data: 20-10-2015

Sommario: **In questo allegato sono riportate le Politiche di sicurezza adottate dall'Ente a cui debbono attenersi responsabili ed incaricati ai trattamenti dei documenti.**

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20/10/2015	Maria Pia Papa	

INDICE

1 PREMESSA

La gestione documentale è un'attività trasversale a tutte le unità organizzative dell'Ente e, pertanto, tutto il personale (impiegati, funzionari e dirigenti) dell'Amministrazione è tenuto, in uno sforzo di squadra, a comportarsi in accordo con le politiche di sicurezza che vengono impartite in questo capitolo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

2 SCOPO

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

3 AMBITO DI APPLICAZIONE

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) che collabora con l'amministrazione e al personale dipendente di ditte che sono autorizzate all'accesso al sistema informativo dell'Ente.

Esse si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

4 POLITICHE – USO GENERALE E PROPRIETA'

Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.

Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

Gli impiegati devono attenersi alle linee guida per l'uso personale di Internet/Intranet/Extranet.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

5 POLITICHE – SICUREZZA E PROPRIETA' DELL'INFORMAZIONE

Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.

Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.

Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "news group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.

Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.

Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

L'Amministrazione adotta specifiche istruzioni operative per la selezione e gestione sicura delle parole chiave.

6 POLITICHE - ANTIVIRUS

6.1 Generalità

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati, capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

E' importante stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet.

Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

6.2 Politiche per le azioni preventive

1. Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
2. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
3. Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
4. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
5. Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
6. Non scaricare mai messaggi da siti o sorgenti sospette.
7. Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
8. Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
9. Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
10. Evitare collegamenti diretti ad Internet via modem.
11. Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
12. Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
13. Non utilizzare i server di rete come stazioni di lavoro.
14. Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.

15. Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno:

1. Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
2. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
3. I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
4. Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico... [omissis]...che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
5. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
6. È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.
7. In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

6.3 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

1. verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
2. verificare se il virus ha diffuso dati;
3. identificare il virus;
4. attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
5. installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
6. diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

7 POLITICHE – USO NON ACCETTABILE

7.1 Generalità

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

7.2 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
    b. attività di "sniffing";
    c. disturbo della trasmissione;
    d. spoofing dei pacchetti;
    e. negazione del servizio;
    f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;

g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

7.3 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

7.4 Uso della posta elettronica e della rete internet

Ai sensi del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007, pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007, questa Amministrazione comunale adotta il "*Disciplinare per l'uso della posta elettronica e della rete internet nel rapporto di lavoro*".

8 POLITICHE - SELEZIONE E GESTIONE SICURA DELLE PAROLE CHIAVE

8.1 Generalità

Tutte le parole chiave a livello di sistema, come ad esempio quelle dell'amministratore di un sistema operativo, devono essere cambiate con una frequenza più elevata, rispetto a quella attribuita a parole chiave conferite ad utenti con profilo di accesso di minore rischio (ogni mese)

Tutte le parole chiave utilizzate a livello di sistema devono essere inserite nel database globale di gestione delle parole chiave.

Tutte le parole chiave attribuite ai singoli incaricati per accedere alla posta elettronica, al proprio computer, ad Internet, eccetera, devono essere cambiate almeno ogni sei mesi. Quest'intervallo di tempo deve essere ridotto a tre mesi, se queste parole chiave vengono utilizzate per accedere a dati personali sensibili e giudiziari.

Si raccomanda, comunque, vivamente di ridurre al massimo questo intervallo di tempo, perché più esso è breve, minori sono le probabilità che la parola chiave venga in qualche modo compromessa.

È fatto assoluto divieto di inserire parole chiave in messaggi di posta elettronica od altre forme di comunicazione elettronica.

8.2 Linee guida per la costruzione delle parole chiave

Le parole chiave possono essere utilizzate per accedere a differenti profili di autorizzazione, nell'ambito del sistema informativo aziendale.

Gli utilizzi più frequenti sono ad esempio: contabilità di utente, accesso ad Internet, accesso a sistemi di posta elettronica, accesso a screen saver, accesso a sistemi di casella elettronica vocale, e simili.

Poiché sono molto rari i sistemi informativi che possono utilizzare parole chiave dinamiche, che vengono usate una volta sola, è indispensabile che ogni incaricato prenda buona nota delle modalità con cui è possibile selezionare parole chiave di difficile individuazione.

8.2.1 Parole chiave deboli

Le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- La parola chiave contiene meno di 8 caratteri, anche se il sistema può accettare parole chiave di 8 caratteri ed oltre;
- La parola chiave si può trovare in un comune dizionario italiano, in inglese od altra lingua comune;
- La parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia;
- Sono da ritenersi insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili;
- Sono inoltre da scartare parole o sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456, eccetera. Sono da scartare parole come sopra, digitate alla rovescia;
- E' da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

8.2.2 Parole chiave sicure

Per contro, sono da ritenersi parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- sono composte da caratteri maiuscoli e minuscoli;
- utilizzano anche caratteri di interpunzione, come; [,] , * " , ed una miscela di numeri e lettere;
- devono avere una lunghezza minima di 8 caratteri alfanumerici, se il sistema consente di raggiungere questa lunghezza;
- non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso;
- non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili;
- un altro importante accorgimento riguarda la selezione di parole chiave che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze.

Le parole sicure non devono mai essere scritte o archiviate in linea.

Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:

1. un primo suggerimento è quello di creare una parola chiave, basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata: ad esempio "tea for two" diventa "teax2";
2. La parola chiave può essere formata abbreviando una intera frase come ad esempio "che gelida manina" diventa "chegemani"

Attenzione: non usare mai alcuno degli esempi sopra illustrati come parola chiave.

8.3 Raccomandazioni per la protezione delle parole chiavi

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'Ente e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività non legate all'attività lavorativa.

Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa parola chiave in relazione a differenti profili (ad esempio, deve essere scelta una parola chiave per l'accesso all'area tecnica del sistema ed una parola chiave separata per l'accesso alla contabilità)

La parola chiave prescelta non dev'essere condivisa con alcun soggetto, interno o esterno all'Ente, ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiavi che sono state generate da un incaricato devono essere trattate come informazione strettamente riservata.

In particolare, ecco un elenco delle cose che non bisogna fare:

1. Non rivelare una parola chiave attraverso il telefono a chicchessia;
2. Non scrivere una parola chiave in un messaggio di posta elettronica;
3. Non rivelare la parola chiave al proprio superiore;
4. Non parlare di parole chiave di fronte a terzi;
5. Non dare alcuna indicazione in merito al formato ed alla lunghezza della parola chiave che si utilizza;
6. Non svelare la parola chiave su questionari o su formulari di sicurezza;

7. Non rivelare la parola chiave a membri della famiglia;
8. Non rivelare la parola chiave ad un proprio collega di lavoro mentre si è in vacanza;

Se qualcuno insiste per conoscere la sua parola chiave con un incaricato, quest'ultimo deve dapprima fare riferimento a questo documento e successivamente informare immediatamente il responsabile della sicurezza logica o il suo titolare o responsabile.

Non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di ricordare la parola chiave.

Non scrivere la parola chiave su un qualsiasi documento e non nasconderlo in alcun posto del proprio ufficio.

Non archiviare la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile, senza utilizzare un algoritmo di cifratura.

Ricordarsi di cambiare la parola chiave almeno una volta ogni sei mesi; quest'intervallo viene ridotto a tre mesi in caso la parola chiave consenta l'accesso al trattamento di dati sensibili e giudiziari.

Se si ha anche solo il minimo sospetto che la propria parola chiave sia stata in qualche modo compromessa o sia venuta a conoscenza di terzi, si provveda immediatamente alla sostituzione della stessa e si riferisca l'accaduto al responsabile della sicurezza logica, oppure al titolare o al responsabile del trattamento di dati personali.

Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il responsabile della sicurezza logica effettui tentativi di violazione della parola chiave di qualche incaricato. Nel caso il tentativo abbia esito positivo, verrà chiesto a costui di sostituire immediatamente la parola chiave.

8.4 Istruzioni speciali per chi gestisce le applicazioni software

I responsabili della gestione delle applicazioni sw devono accertarsi che i loro programmi siano dotati delle seguenti caratteristiche di sicurezza:

- Le applicazioni devono essere in grado di autenticare i singoli individui e non i gruppi;
- Le applicazioni non devono archiviare le parole chiave in chiaro od in una forma facilmente intelligibile;
- Le applicazioni devono avere la possibilità di introdurre la figura di un gestore di livello superiore, di modo che un utente possa subentrare alle funzioni di un altro, senza dover conoscere la sua parola chiave.

8.5 Frasi chiave

Le frasi chiave possono essere utilizzate per l'autenticazione remota di un utente, utilizzando gli algoritmi con chiave pubblica e privata.

Un sistema con chiave pubblica e privata definisce una relazione matematica tra la chiave pubblica, nota a tutti, e la chiave privata, conosciuta soltanto all'utente.

Senza la parola frase che permette di decifrare la chiave privata, l'utente non può ottenere l'accesso al sistema.

Questa architettura di sicurezza è spesso usata in Italia nella gestione di applicativi di firma digitale.

Le frasi chiave non sono la stessa cosa delle parole chiave.

Una frase chiave è una versione più lunga di una parola chiave e quindi più sicura.

Una frase chiave è tipicamente composta da molte parole ed è questa la ragione per cui essa è più sicura contro i cosiddetti "attacchi del dizionario".

Una frase chiave sicura è relativamente lunga e contiene una combinazione di lettere maiuscole e minuscole, nonché numeri e segni di interpunzione. Ecco un esempio di una soddisfacente frase chiave:

"la mattinA e' BELLA"

Tutte le regole prima illustrate, che si applicano alla selezione delle parole chiave, si applicano anche alle frasi chiave.

8.6 Disattivazione del profilo di autenticazione

Nel caso l'incaricato non utilizzi il proprio codice identificativo personale e parola chiave per un periodo superiore a sei mesi, il suo profilo di autenticazione va automaticamente disattivato.

Per riprendere l'operatività, l'incaricato deve prendere contatto con il titolare o responsabile del trattamento di dati personali.

8.7 Disattivazione del profilo di autorizzazione

Per esplicita prescrizione di legge, il profilo di autorizzazione concesso ad un incaricato deve essere verificato almeno una volta l'anno.

È possibile che l'incaricato, pure debitamente autenticato, si trovi impossibilitato ad utilizzare il proprio profilo di autorizzazione, per scadenza dello stesso e mancato rinnovo.

Per riprendere l'operatività, l'incaricato deve prendere contatto con il titolare od il responsabile del trattamento di dati personali.

8.8 Interventi di emergenza

Il disciplinare tecnico in materia di misure minime di sicurezza prevede esplicitamente che sia possibile, per il titolare o il responsabile del trattamento di dati personali, di accedere alla parola chiave di un incaricato, ove per una qualunque ragione egli non sia presente sul posto di lavoro e sorga una urgente esigenza di accedere a dati personali che sono accessibili soltanto con il suo profilo di autorizzazione.

Giova sottolineare che, ove il profilo di autorizzazione sia condiviso con altri soggetti, la procedura di emergenza appresso illustrata non ha ragione di essere utilizzata, in quanto agli stessi dati si può accedere grazie ad un altro incaricato che utilizza la propria parola chiave.

Nel caso il profilo di autorizzazione rientri nella categoria soprariportata, è fatto obbligo all'incaricato di trascrivere la propria parola chiave su un foglio di carta, che deve essere inserito in una busta debitamente sigillata e controfirmata, meglio se chiusa con sigilli inviolabili a numerazione univoca.

Tale busta deve essere consegnata al titolare o al responsabile del trattamento dei dati personali e il suo contenuto deve essere costantemente aggiornato, ogniqualvolta l'incaricato decida di sostituire la propria parola chiave.

È facoltà del titolare o del responsabile, in presenza dell'incaricato, aprire la busta sigillata e verificare che la parola chiave presente sul foglio di carta corrisponda a quella effettivamente in uso.

È fatto obbligo al titolare o al responsabile del trattamento dei dati personali di verbalizzare in apposito registro, con controfirma di garanzia da parte di terzi (precisare), l'avvenuta apertura della busta e la presa di conoscenza della parola chiave.

Resta inteso che dal momento in cui il titolare o il responsabile hanno preso conoscenza della parola chiave, all'incaricato che l'ha selezionata non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati od accessi non consentiti ai dati personali, di cui al suo profilo di autorizzazione.

La sua responsabilità verrà pienamente rimessa in essere non appena l'incaricato avrà avuto la possibilità di selezionare una nuova parola chiave e di assumersi, quindi, nuovamente la piena responsabilità del corretto utilizzo. In tale occasione ci si rammenti di inserire la nuova parola chiave nella busta sigillata, come precedentemente illustrato.

8.9 Sanzioni

Un incaricato che abbia violato queste istruzioni di sicurezza potrebbe essere sottoposto ad azioni disciplinari di vario livello, per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza del sistema informativo comunale.

8.10 Allegati

Moduli	Oggetto
MO – NOMINA CUSTODE PASSWORD	Lettera d'incarico al Custode Password
MO – RICHIESTA PASSWORD	Richiesta Password
MO – COMUNICAZIONE PASSWORD	Comunicazione password

MO – NOMINA CUSTODE PASSWORD

Data _____

Prot. n. _____

Egr. Sig. _____

OGGETTO: LETTERA D'INCARICO AL CUSTODE PASSWORD

Il Sindaco,

visto il D.Lgs 196/03 "Codice in materia di protezione dei dati personali", articoli 33, 34, 35, 36, 180 ed ALLEGATO B,

considerato che

- si evidenzia la necessità di individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, il soggetto preposto alla custodia delle password o che abbia accesso ad informazioni che riguardano le stesse,
- per affidabilità, capacità professionali ed esperienza, Lei fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza;

decreta

di designarLa come soggetto preposto alla custodia delle parole chiave.

Con l'occasione, Le ricordiamo che dovrà usare la massima riservatezza e discrezione nella tenuta delle parole chiave e nella conseguente loro protezione, nel rispetto degli obblighi che Le derivano, previsti dal D. Lgs. 196/03.

Il Titolare del trattamento dei dati

Per accettazione

Data _____

Prot. n. _____

A tutti gli incaricati

OGGETTO: RICHIESTA PASSWORD

La sempre maggiore diffusione di trattamenti informatizzati di documenti e dati e la normativa privacy in vigore (D. Lgs. 196/03), impongono una più razionale e soprattutto sicura gestione degli accessi ai database dell'Ente.

E' necessario, quindi, che tutti gli utenti, attuali e futuri, si attengano alle disposizioni riportate nelle Istruzioni Operative allegate al Piano di Sicurezza: "*Selezione e gestione sicura delle parole chiave*".

Richiesta Password

Con la presente si invita ogni incaricato a fornire la propria password in busta chiusa, richiedendo il modulo per la relativa compilazione a Questo Ufficio.

Conclusioni

Come premesso, le regole sopra citate sono volte a migliorare e garantire la sicurezza degli accessi al Sistema Informativo, pertanto si raccomandano i Signori utenti a coglierne significati e scopi.

Inoltre, è vietato comunicare ai colleghi la propria password: questa prassi non è permessa nel caso in cui l'utilizzo della password del collega è giustificata dal fatto che una funzione procedurale non è presente sul proprio menù, ma su quello del collega stesso. L'utente sprovvisto della funzione interessata dovrà farne richiesta al proprio responsabile.

Qualsiasi variazione riguardante l'abilitazione all'uso dei video terminali e/o personal computers dovrà pervenire a questo ufficio in forma scritta con l'autorizzazione del Responsabile di Settore.

La normativa riguardante le password entrerà in vigore a partire dal ……/……/……..

Il Responsabile della custodia delle password

Per accettazione

MO – COMUNICAZIONE PASSWORD

Data _____

Prot. n. _____

Egr. Sig. _____
Responsabile della custodia
delle Password

OGGETTO: COMUNICAZIONE PASSWORD

Con la presente si comunica la propria password al CUSTODE DELLE PASSWORD, designato da questo Ente:

NOME incaricato del trattamento _____
COGNOME incaricato del trattamento _____
SETTORE di appartenenza _____
SERVIZIO di appartenenza _____

PASSWORD di accensione PC _____
PASSWORD di accesso alla rete _____
PASSWORD Casella di PEC _____
_____ _____
_____ _____

Firma dell'incaricato

N.B. Questo modulo, debitamente compilato, deve essere riconsegnato in busta chiusa con, all'esterno, il nome dell'incaricato. Sarà cura dell'incaricato del trattamento comunicare immediatamente ogni variazione delle proprie password di accesso, utilizzando sempre il presente modulo e le medesime modalità.