COMUNE DI GRIGNASCO

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Ai sensi del decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 –
Regole tecniche per il protocollo informatico ai sensi dell'artt. 40-bis, 41, 47, 57-bis e 71 del C.A.D. di cui D.L. 82/2005

INDICE

1 PRINCIPI GENERALI

1.1 Premessa

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti interni e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.
Il protocollo informatico costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione. Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce indicazioni complete circa la corretta esecuzione delle operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti informatici. Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.
Esso disciplina:

- la gestione dei documenti in un contesto di dematerializzazione e di digitalizzazione dei procedimenti;
- i livelli di esecuzione, le responsabilità e i metodi di controllo dei processi e delle azioni amministrative;
- le modalità operative di gestione del protocollo, dei flussi documentali e procedimentali, degli archivi;
- l'uso del titolario di classificazione e del piano di fascicolazione;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa;

1.2 Ambito di applicazione del manuale

Il presente Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi è adottato ai sensi del decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71 del C.A.D. di cui D.L. 82/2005. Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali dell'Ente.
Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa. Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3 Definizioni

Ai fini del presente Manuale si intende:

• per "CAD", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale, nel testo vigente.
• per "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi dell'artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui D.L. 82/2005.

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea;
- PdP - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- UO – Unità Organizzativa – unità organizzativa interna (settore, servizio, ufficio)
- UCP - Unità Organizzativa Centrale di registrazione di Protocollo – rappresenta l'ufficio centrale di protocollo
- UOP – Unità Organizzativa di registrazione di Protocollo – unità organizzativa abilitata alla protocollazione, diversa dall'ufficio centrale di protocollo.
- UOR - Uffici Organizzativi di Riferimento - un 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;
- RPA Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- RSP - Responsabile della gestione documentale e del Servizio di Protocollo informatico;
- MdG - Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi;

1.4 Norme di riferimento

Le principali norme di riferimento sono elencate nell'allegato 1 - Norme di riferimento"

2 DOCUMENTI E MODALITA' DI GESTIONE

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

- informatico ("rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti");
- analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").

In termini operativi, il documento amministrativo è invece classificabile in:

- ricevuto;
- inviato;

- interno formale
- interno informale

2.1 Il documento informatico amministrativo

Il Codice dell'Amministrazione Digitale definisce il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.
Secondo quanto previsto dall'art. 40 del CAD "1. Le pubbliche amministrazioni 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".

2.2 Il documento analogico – cartaceo amministrativo

Per documento analogico si intende " la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" cioè un documento "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, 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 predisposto con strumenti informatici (ad esempio, una lettera prodotta tramite un software di office automation) e poi stampato.
In quest'ultimo caso si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa.

2.3 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, a titolo esemplificativo:

- a mezzo posta elettronica convenzionale o certificata;
- su supporto rimovibile quale, ad esempio, CD ROM, DVD, floppy disk, pen drive, hard disk esterni, etc, consegnato direttamente o inviato per posta convenzionale o corriere;
- tramite portale/spazio web dedicato.

Un documento analogico può essere tipicamente recapitato:
• a mezzo posta convenzionale o corriere;
• a mezzo posta raccomandata;
• per telefax o telegramma;
• con consegna diretta a una delle unità organizzative aperte al pubblico da parte dell'interessato o di persona delegata.
L'Ente dà piena attuazione a quanto disposto dall'art. 45, comma 1, del CAD, in base al quale "I documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale".

2.4 Documento inviato

I documenti informatici, con gli eventuali allegati, anch'essi informatici, sono inviati di norma per mezzo della posta elettronica convenzionale o certificata.
Il documento informatico può inoltre essere riversato su supporto digitale rimovibile in formato non modificabile, per la trasmissione al destinatario con altri mezzi di trasporto.
Lo scambio di documenti con altre Pubbliche Amministrazioni avviene prioritariamente mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa.

2.5 Documento interno formale

I documenti interni sono formati con tecnologie informatiche avvalendosi del sistema di scrivania e gestione documentale.
Il documento informatico di rilevanza amministrativa giuridico-probatoria scambiato tra unità organizzative mediante il sistema di gestione documentale viene preventivamente sottoscritto con firma digitale o altra firma elettronica. Il sistema in uso è in grado di tracciare in modo immodificabile tutte le operazioni relative a una registrazione, con un meccanismo di attribuzione alla singola persona di documenti o annotazioni che configura i requisiti per l'identificazione informatica.

2.6 Documento interno informale

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

2.7 Copia informatica di documento analogico

La copia informatica di documento analogico viene formata mediante copia per immagine (scansione di documento amministrativo cartaceo o altra modalità) che genera un documento informatico con **contenuto e forma identici** a quelli dell'originale analogico.
La copia ha la stessa efficacia probatoria dell'originale da cui è tratta se la conformità all'originale non è espressamente disconosciuta.
La dichiarazione di conformità all'originale:
- Certifica il processo di formazione della copia che garantisce la corrispondenza di forma e contenuto di originale e copia
- E' attestata dal funzionario delegato dal Sindaco ad autenticare le copie
- E' sottoscritta con firma digitale (in quanto sostituisce anche il timbro)
- Può essere inserita nel documento informatico contenente la copia informatica oppure può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia.

Formule

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

2.8 Copia analogica di documento informatico

La copia analogica (cartacea) di documento informatico formata mediante il sistema di gestione documentale, conforme alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014) ha la stessa efficacia probatoria dell'originale da cui è tratta se la conformità all'originale non è espressamente disconosciuta.

La copia riporta in calce l'indicazione della conformità del sistema alle regole tecniche vigenti.

Formula

Copia analogica di documento informatico prodotta con sistema di gestione documentale conforme alle regole tecniche vigenti (D.P.C.M. 14 novembre 2014)

Se la copia analogica (cartacea) di documento informatico è formata al di fuori del sistema di gestione documentale, la conformità viene attestata con apposita dichiarazione in calce alla copia, sottoscritta con firma autografa dal funzionario delegato dal Sindaco ad autenticare le copie.

Formula

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

2.9 Duplicati di documenti informatici

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

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

I duplicati prodotti dal presente sistema di gestione documentale, conforme alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014), sono costituiti dalla la stessa sequenza di bit del documento informatico di origine e pertanto hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti.

Se i duplicati non sono prodotti dal sistema di gestione documentale, ai duplicati viene allegata un'attestazione di conformità relativa al processo di formazione del duplicato che assicura l'identità della sequenza di bit del duplicato rispetto all'originale.

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

2.10 Copie ed estratti informatici di documenti informatici

La copia e gli estratti informatici dei documenti informatici sono prodotti attraverso il sistema di gestione documentale che utilizza i formati esposti nell'apposito allegato, nonché mediante processi e strumenti che assicurano la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine. In tal caso copie ed estratti hanno la stessa efficacia probatoria dell'originale se la conformità non è espressamente disconosciuta. La copia e l'estratto riportano la seguente formula:

Copia/estratto di documento informatico prodotto con sistema di gestione documentale conforme alle regole tecniche vigenti (D.P.C.M. 14 novembre 2014)

Se la copia e gli estratti informatici dei documenti informatici non sono prodotti attraverso il sistema di gestione documentale, in calce alle copie ed estratti informatici viene inserita l'attestazione di conformità all'originale delle copie o dell'estratto informatico sottoscritta con firma digitale dal funzionario delegato dal Sindaco.

Il sottoscritto, nella sua qualità di funzionario delegato dal Sindaco, attesta che la copia / estratto informatico sopra riportato è conforme all'originale informatico.. Il Funzionario Incaricato Firma digitale

2.11 Formazione del documento informatico

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 deve:

- trattare un unico argomento indicato in maniera sintetica, ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;
- fare riferimento, in via principale, ad un solo fascicolo.

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

L'art. 3 del DPCM del 13 novembre 2014 evidenzia che:

1. Il documento informatico e' 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.

2. Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

3. Il documento informatico, identificato in modo univoco e persistente, e' memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.

4. Nel caso di documento informatico formato ai sensi del comma 1, lettera a), le caratteristiche di immodificabilità e di integrità sono determinate da una o giù delle seguenti operazioni:
   a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
   b) l'apposizione di una validazione temporale;
   c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
   d) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
   e) il versamento ad un sistema di conservazione.

5. Nel caso di documento informatico formato ai sensi del comma 1, lettera b), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di

gestione informatica dei documenti che garantisca l'inalterabilità' del documento o in un sistema di conservazione.

6. Nel caso di documento informatico formato ai sensi del comma 1, lettere c) e d), le caratteristiche di immodificabilita' e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

7. Laddove non sia presente, al documento informatico immodificabile è associato un riferimento temporale.

8. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 4 del presente decreto in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità. Formati diversi possono essere scelti nei casi in cui la natura del documento informatico lo richieda per un utilizzo specifico nel suo contesto tipico.

9. Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'allegato 5 al presente manuale, è costituito da:

    a) l'identificativo univoco e persistente;
    b) il riferimento temporale di cui al comma 7;
    c) l'oggetto;
    d) il soggetto che ha formato il documento;
    e) l'eventuale destinatario;
    f) l'impronta del documento informatico.

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

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

2.12 La firma

Nell'ambito del sistema di gestione documentale questo Ente utilizza le seguenti tipologie di firma:

Semplice: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica in forma di PIN o insieme di Username e Password.
La firma semplice viene utilizzata per l'autenticazione a fini di consultazione e accesso all'erogazione di servizi:

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

Non ha valore di sottoscrizione.
La firma semplice viene rilasciata a tutti gli operatori del sistema di gestione documentale.

Firma avanzata: consente l'identificazione del firmatario e la connessione univoca ad esso. Le forme di firma avanzata utilizzabili da questo Ente sono: Certificati digitali, codici OTP (One Time Password), firma grafometrica, PEC con ricevuta completa, Carta Naz. Servizi.
Nei rapporti con i soggetti esterni, segnatamente in caso di ricezione dei documenti la firma avanzata per così dire "sostitutiva" rappresentata dalla ricevuta completa della PEC, costituisce legittimazione per l'inserimento all'interno di un'istruttoria procedimentale di documentazione prodotta dal mittente interessato al procedimento.
All'interno dell'Ente la firma avanzata viene utilizzata come sistema di validazione di fasi procedimentali, di comunicazione interna, di abilitazione allo svolgimento di attività specifiche.
Non ha valore di sottoscrizione con rilevanza esterna.
La firma avanzata viene rilasciata a tutti gli operatori del sistema di gestione documentale.

Firma qualificata: realizzata mediante dispositivo sicuro per la generazione di un certificato digitale e utilizzata mediate dispositivi quali Token, Smart card, Firma remota, Firma automatica.
Viene utilizzata per tutte le attività di natura pubblicistica che non richiedono che il documento informatico acquisisca le caratteristiche di immodificabilità ed integrità ed inoltre che non richieda l'apposizione di timbri o sigilli.
La firma avanzata viene rilasciata a tutti i Responsabili di procedimento e tutti gli operatori legittimati alla sottoscrizione di documenti aventi rilevanza esterna.

Firma digitale: costituita da un certificato qualificato e sistema di chiavi crittografiche, una pubblica e una privata, consente di rendere manifesta e di verificare la provenienza e l'integrità di uno o più documenti informatici . Si utilizza con dispositivi quali token, smart card, firma remota e firma automatica.
In relazione al valore legale di firma autografa e sottoscrizione, garantisce, oltre alla provenienza, anche l'integrità e l'autenticità del documento sottoscritto, inoltre sostituisce l'apposizione di timbri e sigilli.
Viene utilizzata per la firma di provvedimenti con effetto costitutivo, modificativo o estintivo di rapporti giuridici, sia di natura pubblicistica (delibere, decreti, determinazioni, ordinanze, buoni di ordinazione, ordinativi di incasso e pagamento, documenti finanziari e contabili, pareri etc) che privatistica e contrattuale (contratti, ordini, contabilizzazioni di lavori pubblici) che verranno versati nel sistema di conservazione.
La firma digitale viene rilasciata a tutti i Responsabili di procedimento anche con delega all'adozione di provvedimenti, ai Responsabili di Servizio e tutti gli operatori legittimati alla sottoscrizione di documenti aventi rilevanza esterna.

Firma autografa: su documenti analogici e copie analogiche di documenti informatici.

2.13 Autenticazione firma

L'autenticazione delle firme è prevista per la firma elettronica o qualsiasi altro tipo di firma avanzata (FEA, qualificata e digitale) e viene effettuata da un pubblico ufficiale (Segretario Comunale o funzionario delegato dal Sindaco) che attesta, firmando con firma digitale, che

a) la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale,
b) il eventuale certificato elettronico utilizzato è valido
c) il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

L'autenticazione avviene anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata
Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata.

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

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

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

Con riferimento in particolare a documenti specifici quali:

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

Il documento, una volta divenuto immodificabile, deve essere associato l'insieme minimo dei metadati (identificativo univoco e persistente,il riferimento temporale , l'oggetto, il soggetto che ha formato il documento, l'eventuale destinatario, l'impronta informatica). Eventuali ulteriori metadati sono descritti nell' allegato 5.

2.15 Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno della AOO;
- l'interconnessione tra le unità organizzative della AOO nel caso di documenti interni;
- la certificazione dell'avvenuto inoltro e ricezione.

2.16 Trasmissione documenti con il sistema pubblico di connettività

Lo scambio dei documenti informatici tra le varie amministrazioni, e con i cittadini, avviene attraverso meccanismi di "interoperabilità" e "cooperazione applicativa". L'articolo 72 del CAD, distinguendo due diversi livelli di interoperabilità, ne fornisce la seguente definizione:

- interoperabilità di base: i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;
- interoperabilità evoluta: i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;
- cooperazione applicativa: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Il rispetto degli standard di protocollazione e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo.

L'interoperabilità e la cooperazione applicativa tra le Amministrazioni Pubbliche sono attuate attraverso una infrastruttura condivisa a livello nazionale, operante sul Sistema Pubblico di Connettività (SPC), che si colloca nel contesto definito dal CAD. Quest'ultimo definisce il SPC come "insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza,

la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione."

2.17 Uso della Posta Elettronica Certificata

L'utilizzo della Posta Elettronica Certificata (PEC) o di altro sistema analogo consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La dichiarazione da parte dell'utente del proprio indirizzo di posta elettronica certificata costituisce espressa accettazione dell'invio, tramite questo canale, degli atti e dei provvedimenti amministrativi relativi all'utente stesso. Quanto sopra vale anche per l'indirizzo di posta elettronica ordinaria, per le istanze, le comunicazioni e le dichiarazioni presentate all'Ente. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta raccomandata, salvo che la legge disponga diversamente.

L'AOO dispone di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento.

2.18 Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti.
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
I sistemi di gestione informatica dei flussi documentali, orientati alla trasparenza amministrativa ed all'efficienza interna, si collocano in una dimensione più ampia nell'ottica della interconnessione e interoperabilità dei sistemi informativi pubblici.

Per interoperabilità dei sistemi di gestione documentale e protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema, delle informazioni trasmesse da un diverso sistema mittente, allo scopo di automatizzare altresì le attività ed i processi amministrativi conseguenti (art. 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Per realizzare l'interoperabilità dei sistemi di gestione documentale e protocollo informatico gestiti dalle pubbliche amministrazioni distribuite sul territorio è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Alla luce del decreto Legislativo 7 marzo 2005, n. 82, (di seguito CAD), i mezzi di comunicazione telematica di base, sono costituiti dalla:
- posta elettronica e posta elettronica certificata, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi secondo quanto indicato nelle regole tecniche per il protocollo informatico previste dal CAD (di seguito regole tecniche);
- cooperazione applicativa basata sul Sistema Pubblico di Connettività (di seguito SPC) e Sistema Pubblico di Cooperazione (di seguito SPCoop). In tale caso i messaggi scambiati tra Enti e PA attraverso le Porte di Dominio, secondo gli standard definiti nell'ambito dell'SPCoop, sono racchiusi in una busta (di seguito Busta di e-Gov) costituita da un uso della struttura SOAP 1.1 con estensioni (come indicato nelle regole tecniche del SPC di cui al D.P.C.M. 1 aprile 2008).

Oltre ad una modalità di comunicazione comune, l'interoperabilità dei sistemi di protocollo richiede anche una efficace interazione dei sistemi di gestione documentale. In questo senso, le regole tecniche stabiliscono che ogni messaggio protocollato debba riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato.
Secondo quanto previsto nelle regole tecniche, con il presente documento, reso disponibile anche sul sito web dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.
Le modalità tecniche ed il formato definiti verranno adeguati in relazione all'evoluzione tecnologica e alle eventuali ulteriori esigenze che le amministrazioni dovessero manifestare a seguito della loro applicazione.

3 ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

3.1 Il protocollo informatico

L'Ente gestisce un unico protocollo informatico per tutti i documenti in arrivo e in partenza nell'ambito di un sistema di gestione documentale conforme alle previsioni di cui

- alle Regole Tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57 bis e 71 del Codice dell'Amministrazione digitale di cui al D.Lgs n. 82/2005 (di segui indicato come Codice) approvate con D.P.C.M. 3 dicembre 2013 (di seguito indicate come Regole Tecniche)
- al Testo Unico sulla documentazione amministrativa approvato con D.P.R. 445/2000 (di seguito indicato come TU).

Il registro è generato automaticamente dal sistema di protocollo che assegna a ciascun documento registrato il numero e la data di protocollazione.
All'unico sistema di protocollazione corrisponde un unico titolario di classificazione.
L'Ente produce un unico archivio, l'articolazione in archivio corrente, archivio di deposito ed archivio storico risponde esclusivamente a criteri di funzionalità.
I responsabili dei procedimenti amministrativi dei singoli uffici provvedono alla implementazione della fascicolazione della corrispondenza in arrivo ed alla protocollazione della corrispondenza in partenza. Gestiscono e custodiscono i documenti dell'archivio corrente (e, in alcuni casi, dell'archivio di deposito).

Nell'ambito della gestione documentale il sistema di protocollo si compone di:

- risorse archivistiche: piano di classificazione o titolario (Allegato 3) e presente manuale di gestione
- risorse informatiche: software applicativo dedicato descritto nell'apposito (Allegato 7), piattaforma documentale, PEC e posta elettronica ordinaria, cooperazione applicativa tra Pubbliche Amministrazioni, piattaforme di interscambio;
- risorse umane: operatori del servizio, responsabile della gestione documentale, coordinatore della gestione documentale (Allegato 2)
- risorse normative: D.P.R. 445/2000, D.P.C.M. 3 dicembre 2013, D.Lsg 82/2005, il presente manuale.

3.2 Aree Organizzative Omogenee e modelli organizzativi

L'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) che è composta dall'insieme di tutte le unità organizzative (settori, servizi, uffici). All'interno della AOO il sistema di protocollazione è unico.
Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. All'interno della AOO il sistema di protocollazione è parzialmente centralizzato per la corrispondenza in entrata mentre è decentralizzato per la corrispondenza in uscita, attraverso tutte le unità organizzative che svolgono anche i compiti di UOP.

Gli operatori incaricati dell'attività di protocollazione sono abilitati dal Responsabile della gestione documentale e del Servizio di Protocollo informatico che ha anche il compito di vigilare sulla corretta esecuzione delle attività.
L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le informazioni che individuano l'amministrazione stessa e le unità organizzateive in cui è articolata.

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'amministrazione 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 tutti i dati. Per maggiori dettagli si rimanda alle sezione 3.3 del presente manuale di gestione

3.3 Accreditamento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA)

Nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;
- l'indirizzo della sede principale della amministrazione;
- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:
  - – della denominazione;
  - – del codice identificativo;
  - – della casella di posta elettronica;
  - – del nominativo del RSP;
  - – della data di istituzione;
  - – dell'eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'AOO.
- i dati relativi alla fatturazione elettronica
- ...

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

3.4 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico

Nell'AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Alla guida del suddetto servizio è posto il Responsabile della gestione documentale e del Servizio di Protocollo informatico (RSP). La nomina è riportata nell'allegato 2 del presente manuale.
Il Responsabile è funzionalmente individuato nella figura del Responsabile DELL'Area amministrativa. In caso di assenza del Responsabile, le sue funzioni sono demandate al vicario formalmente delegato.
E' compito del Responsabile:

- provvedere all'aggiornamento e all'eventuale revisione del Manuale della gestione documentale e del Servizio di Protocollo informatico;

- provvedere alla pubblicazione e divulgazione del Manuale, anche attraverso il sito Internet dell'Amministrazione;
- abilitare gli addetti dell'amministrazione all'utilizzo del sistema software di gestione documentale e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.) e l'ambito di azione consentito;
- verificare il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- supervisionare la corretta produzione del registro giornaliero di protocollo curata dall'ufficio protocollo;
- supervisionare la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard ammessi dalla normativa vigente;
- la supervisione dell'invio del pacchetto di versamento che sarà formato dai delegati di ogni unità organizzativa dell'AOO e quindi del transito del pacchetto al sistema di conservazione. Il documento, il fascicolo o l'aggregazione per poter essere correttamente versati in conservazione devono essere stati formati e gestiti in ottemperanza alle regole tecniche sulla formazione, protocollazione e firma secondo le regole tecniche e secondo quanto esplicitato nel presente manuale.
- proporre eventuali modifiche al Titolario di classificazione;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e comunque in conformità a quanto stabilito nel Piano di continuità operativa/DR e relativi allegati;
- 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;
- supervisionare il buon funzionamento degli strumenti e curare 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.

3.5 La classificazione dei documenti

La classificazione è un'attività di organizzazione logica di tutti i documenti correnti, protocollati e non (spediti, ricevuti, interni) secondo uno schema di voci che identificano attività e materie specifiche del soggetto produttore.
Il sistema complessivo di organizzazione dei documenti è definito nel titolario di classificazione.
Lo scopo del titolario di classificazione è quello di guidare la sedimentazione dei documenti secondo le funzioni del soggetto. La classificazione collega ciascun documento in maniera univoca ad una precisa unità archivistica, il fascicolo

3.6 Requisiti minimi di sicurezza dei sistemi di gestione documentale e protocollo informatico

1. Il sistema di gestione documentale e 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.
   e) l'univoca identificazione dei documenti;

2. Il sistema di gestione documentale e protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
3. Il sistema di gestione documentale e 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.

3.7 Tutela dei dati personali

L'amministrazione, titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza, dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.
Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e gestione documentale, sono formalmente incaricati.
Relativamente agli adempimenti esterni, l'Amministrazione si è organizzata per garantire che i certificati e i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite. Inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente. Di norma l'interfaccia di accesso viene configurata in modo da inglobare tali limitazioni, prevenendo così alla fonte eventuali accessi illeciti o eccedenti le effettive necessità.
Viene quindi garantito il diritto dei cittadini e delle imprese ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

3.8 Formazione del personale

Nell'ambito delle attività di attivazione ed applicazione del sistema di gestione documentale e di workflow, l'Ente organizza percorsi formativi specifici e generali che coinvolgono il personale.
In particolare, considerato che il personale assegnato al servizio di protocollo deve conoscere sia l'organizzazione e i compiti svolti da ciascuna unità organizzativa all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, vengono effettuati percorsi formativi e di aggiornamento volti ad assicurare l'operatività del personale stesso.

4 DESCRIZIONE DEL FLUSSO DI ELABORAZIONE DEI DOCUMENTI

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

4.1 Generalità

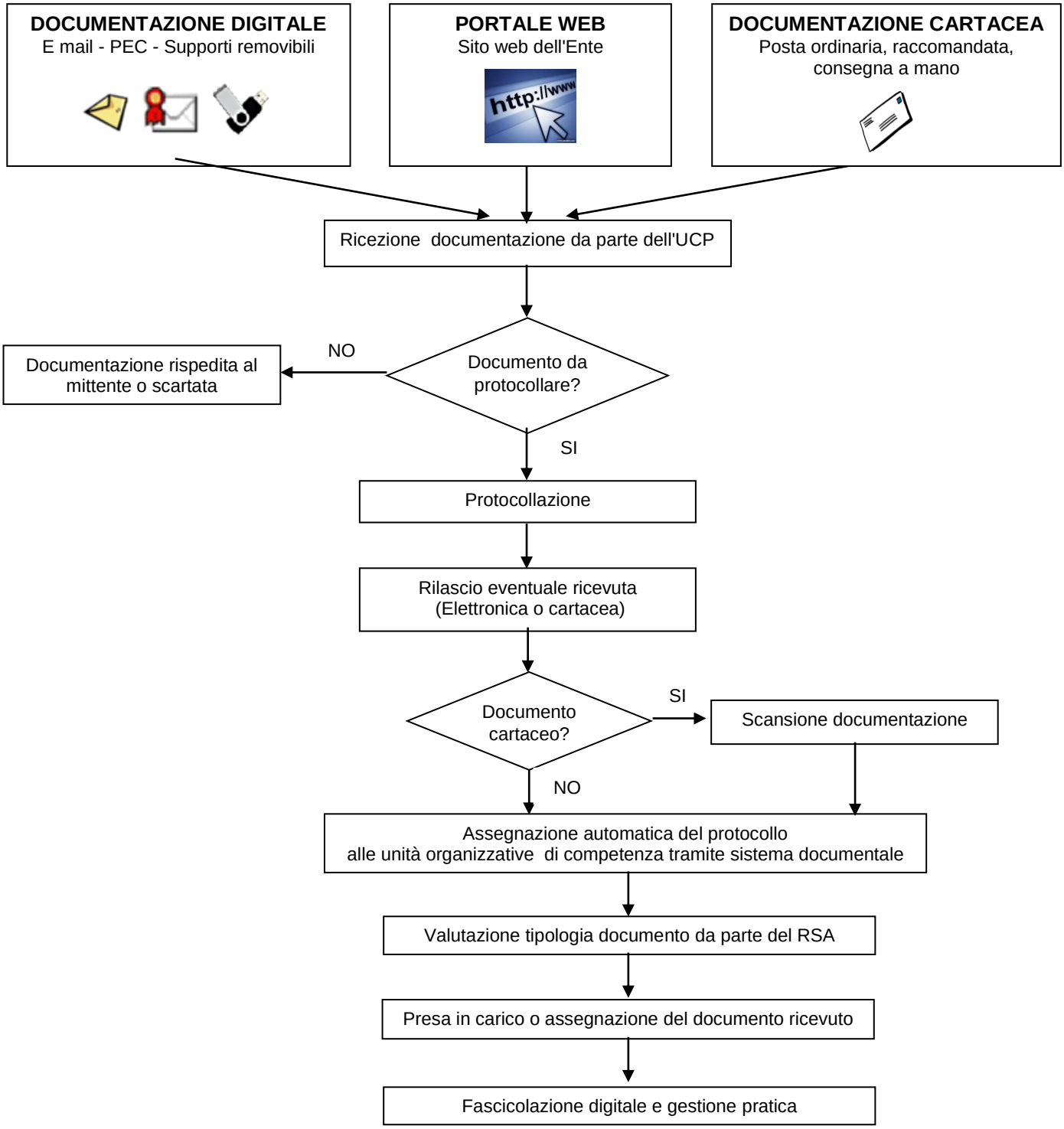
Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.
Essi si riferiscono, in particolare, ai documenti:

- ricevuti dalla AOO, dall'esterno
- inviati dalla AOO, all'esterno

La schematizzazione relativa ai documenti ricevuti si riferisce ad un flusso di lavoro ove la maggior parte delle operazioni sono gestite dall'ufficio protocollo.
L'avvio effettivo del procedimento collegato alla documentazione protocollata viene gestita dalle singole unità organizzative competenti

La schematizzazione relativa ai documenti inviati si riferisce ad un flusso di lavoro svolto prevalentemente dall'unità organizzativa competente.

4.2 Flusso dei documenti ricevuti dalla AOO



4.2.1 Ricezione di documenti informatici sulle caselle di posta elettronica certificata

Di norma la ricezione dei documenti informatici è assicurata tramite le caselle di posta elettronica certificata.

Tale modalità rappresenta la norma anche per la ricezione dei documenti per i quali è richiesta la pubblicazione all'Albo Pretorio on line dell'Ente.
Ogni messaggio deve riferirsi a una sola questione. Anche nel caso in cui vengano inviati contestualmente più documenti, deve essere possibile attribuire all'invio una unica protocollazione, e una unica classificazione.
Quando i documenti informatici pervengono all' ufficio protocollo (o ad altro servizio tramite la propria casella di posta elettronica certificata) la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.
Le caselle PEC sono controllate quotidianamente, nel giorni di apertura degli uffici, dalla UCP o dai singoli servizi.
I documenti ricevuti per via telematica sono resi disponibili agli uffici attraverso il sistema di gestione documentale adottato dall'Ente subito dopo l'operazione di classificazione e smistamento.

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica tradizionale

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non destinata specificamente al servizio di protocollazione e non PEC o similare, spettano al titolare della casella le valutazioni e le incombenze in merito alla ricevibilità, alla protocollazione e classificazione dello stesso con inserimento nel sistema comunale di gestione documentale. I documenti pervenuti tramite fax server ad indirizzi diversi da quello assegnato alla UCP sono trattati con gli stessi criteri indicati per la posta elettronica tradizionale. A ogni messaggio di posta elettronica corrisponde una unica operazione di registrazione di protocollo. Quest'ultima si può riferire sia al corpo del messaggio, sia a uno o più file allegati.
Le comunicazioni pervenute da altre amministrazioni, attraverso gli stessi canali, sono considerate valide ai fini del procedimento amministrativo se è possibile accertarne la provenienza, in conformità a quanto previsto dall'art. 47 del CAD.

4.2.3 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati su supporti rimovibili. L' AOO si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a verificare, decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase, il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

4.2.4 Ricezione di documenti informatici da portale web dell'Ente

I documenti digitali possono anche essere ricevuti dall'Ente dal sito internet istituzionale, tramite apposito servizio web. Il cittadino, dopo essersi registrato al servizio, può avviare on line la procedura di erogazione dei servizi messi a disposizione dall'Ente. Al termine dell'operazione, verrà rilasciata all'utente una ricevuta attestante l'avvenuta presa in carico della sua richiesta.

4.2.5 Ricezione di documenti cartacei a mezzo servizio postale, corriere o consegnati a mano

I documenti pervenuti a mezzo posta convenzionale o tramite corriere sono consegnati all'ufficio protocollo. I documenti consegnati a mano agli uffici comunali sono verificati ed eventualmente consegnati all'ufficio protocollo che provvede alla protocollazione e correttamente inseriti nel sistema di gestione documentale.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.
La corrispondenza cartacea relativa a bandi di gara è registrata (con scansione della busta, e annotazione dell'orario preciso di ricezione ove richiesto) e successivamente consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza personale non deve essere aperta, né protocollata: deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, consegnata all'ufficio protocollo per la registrazione e le operazioni complementari alla stessa. Quando la corrispondenza non rientra nelle categorie da ultimo 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.
Le ricevute di ritorno della posta raccomandata potranno essere scansionate ed inserite nel sistema di gestione documentale collegate al relativo fascicolo/procedimento.

4.2.6 Corrispondenza di particolare rilevanza e documenti esclusi

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

Sono esclusi dalla registrazione di protocollo:

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

Altre categorie documentali potranno essere escluse dalla protocollazione, su disposizione del Responsabile della gestione documentale e del Servizio di Protocollo informatico debitamente comunicata a tutti gli interessati. Al di fuori di queste categorie, non sono ammesse eccezioni all'obbligo di protocollazione, segnatura e corretta gestione dei documenti.

4.2.7 Errata ricezione di documenti digitali

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

4.2.8 Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente all'Ente documenti indirizzati ad altre Amministrazioni o soggetti, possono verificarsi le seguenti eventualità:

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

4.2.9 Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti attraverso la casella di posta certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.
Nel caso di invio documentazione tramite servizi on line sul portale dell'Ente viene automaticamente rilasciata dal sistema una ricevuta attestante l'invio della documentazione.
Nel caso di documenti inviati via posta elettronica certificata per la pubblicazione all'Albo pretorio Comunale, la conferma di pubblicazione (se richiesta) potrà essere trasmessa al mittente attraverso lo stesso canale, immediatamente dopo la scadenza della pubblicazione richiesta.
Nessuna ricevuta viene di norma rilasciata o trasmessa in caso di ricezione di documenti tramite posta elettronica tradizionale, salvo specifica richiesta.

4.2.10 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alla protocollazione in arrivo non rilasciano, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. Sono di regola esclusi dalla protocollazione i documenti non indirizzati all'Ente, per i quali lo stesso funge unicamente da tramite tra il mittente e il destinatario finale.
Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all' ufficio protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'ufficio rilascia una ricevuta generata automaticamente dal sistema di protocollo oppure può essere rilasciata copia della prima pagina del documento (o fotocopia della busta chiusa) riportante il timbro o l'etichetta con gli estremi della segnatura.
Nel caso di istanze che diano avvio a un procedimento, in luogo del suddetto documento viene rilasciata una "ricevuta di presentazione/comunicazione di avvio del procedimento", riportante tutte le indicazioni richieste dalla normativa vigente.

4.2.11 Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla protocollazione, per i documenti da loro trattati, eseguono di norma la classificazione sulla base del Titolario di classificazione adottato presso l'AOO e provvedono ad inviarli tramite il sistema documentale all'unità organizzativa di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, ritrasmette il documento all'ufficio protocollo;
- in caso di verifica positiva, esegue l'operazione di presa in carico e fascicolazione digitale;
- assegna le eventuali visibilità ulteriori rispetto a quelle attribuite automaticamente in base alla classificazione;
- gestisce il documento

Terminata la fase di protocollazione, i documenti sono portati automaticamente nella disponibilità dei soggetti competenti alla loro trattazione grazie al sistema documentale adottato dall'Ente. Il sistema consente comunque di assegnare la visibilità dei documenti ad altri soggetti singoli, uffici o gruppi trasversali di addetti configurati sul sistema. Questa modalità operativa consente di portare il documento all'attenzione di tutti i soggetti interessati, attraverso la condivisione interna del sistema documentale. Si tratta di una modalità particolarmente utile per favorire la conoscenza, e la disponibilità diffusa, di tipologie documentali quali circolari, manualistica, disposizioni operative, documenti di interesse generale ecc.
Viceversa, i documenti risultano inesistenti per i soggetti ai quali non è stata assegnata, automaticamente o meno, la visibilità specifica. Si tratta di un meccanismo semplice ed affidabile per garantire la corretta gestione dei documenti riservati, contenenti dati sensibili o giudiziari, o comunque particolarmente delicati.

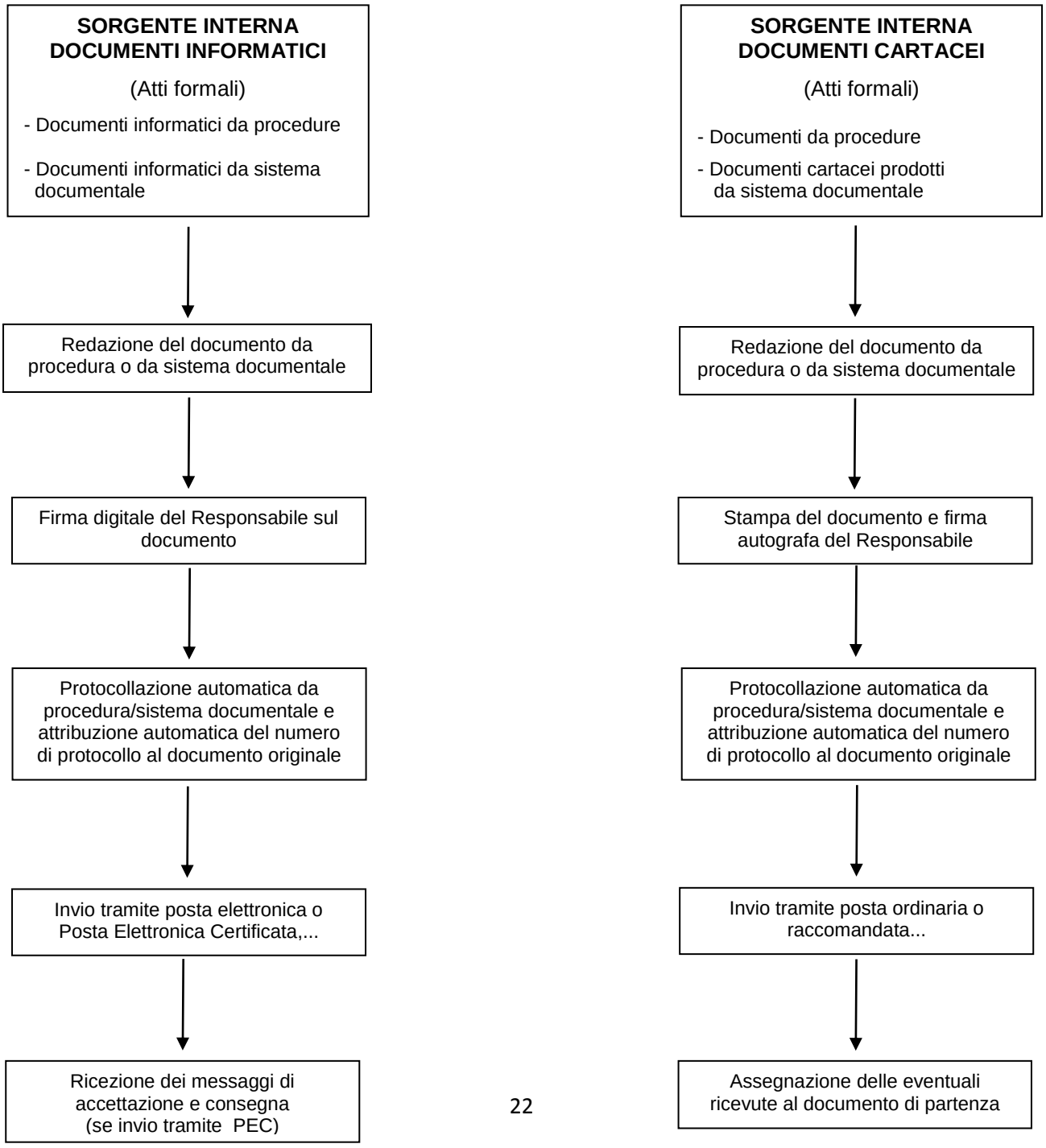
Nel caso di assegnazione errata, l'unità organizzativa che riceve il documento comunica l'errore all'ufficio protocollo che ha assegnato il documento, affinché proceda ad una nuova assegnazione

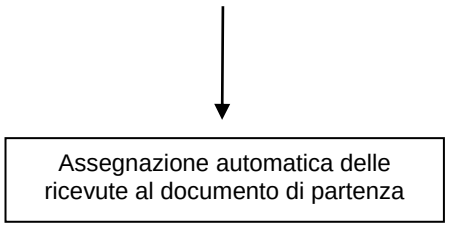
Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'unità organizzativa competente attraverso il sistema di gestione documentale al termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione.

I documenti ricevuti dall'amministrazione in formato cartaceo, di regola acquisiti in formato immagine o altro formato standard non modificabile con l'ausilio di scanner, una volta concluse le operazioni di registrazione segnatura e assegnazione sono fatti pervenire al Servizio di competenza per via informatica attraverso il sistema di gestione documentale. L'originale cartaceo viene anch'esso trasmesso alla struttura di competenza, mediante collocazione nell'apposita cartella presso l'Ufficio Protocollo.

L'unità organizzativa competente ha notizia dell'arrivo del documento tramite apposita "notifica" generata automaticamente dal sistema documentale.

4.3 Flusso dei documenti creati e trasmessi dall'AOO





4.3.1 Sorgente interna dei documenti

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria e destinati ad essere trasmessi a soggetti esterni all'Amministrazione.
Il documento viene predisposto in formato digitale, secondo gli standard illustrati nei precedenti capitoli, e recapito prioritariamente tramite posta elettronica certificata.
I documenti vengono prodotti con il sistema documentale in dotazione all'Ente con le modalità descritte nell'allegato 7

Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere riprodotto in formato analogico. Il mezzo di recapito della corrispondenza, in quest'ultimo caso, è tipicamente costituito dal servizio postale, nelle sue diverse forme.

4.3.2 Verifica formale dei documenti

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

4.3.3 Registrazione di protocollo e segnatura

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

4.3.4 Trasmissione di documenti informatici

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.
Per la spedizione dei documenti informatici, l'AOO si avvale prioritariamente di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, e di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche. In particolare, la PEC è strumento ordinario di trasmissione verso i cittadini che hanno dichiarato il loro domicilio digitale, nonché verso i soggetti inseriti nell'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti, o in altri indici analoghi che si rendessero disponibili in futuro.
In caso di più destinatari riferiti a un unico numero di protocollo, si generano tante PEC quanti sono i destinatari.

E’ ammesso il recapito tramite posta elettronica tradizionale, qualora si disponga dei necessari riferimenti relativi al destinatario.
Nel caso di trasmissione di allegati al documento che eccedano la capienza della casella di posta elettronica, è possibile utilizzare supporti rimovibili, o avvalersi di adeguati canali telematici alternativi.
La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene sempre, ove tecnicamente possibile, mediante posta elettronica certificata, con effetto equivalente alla notificazione per mezzo della posta raccomandata.

4.3.5 Trasmissione di documenti cartacei a mezzo posta

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

4.3.6 Conteggi e spedizione corrispondenza cartacea

L'ufficio protocollo effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza cartacea e cura il costante monitoraggio della spesa e verifica la disponibilità delle necessarie risorse economiche, informando con congruo anticipo il RSP dell’imminente esaurimento dei fondi a disposizione.
Il Responsabile della gestione documentale e del Servizio di Protocollo informatico promuove l’utilizzo di strumenti alternativi al servizio postale (e-mail, e-mail certificata ecc.) presso gli uffici comunali.

4.4 Documenti informali

Si considerano documenti informali i documenti che non assumono rilievo all'interno di procedimenti (informazioni etc).
Gli scambi di documenti informali, all'interno dell'AOO o verso l'esterno, non danno luogo a protocollazione

5 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE DIGITALE E ARCHIVIAZIONE

Il presente capitolo illustra il sistema di classificazione dei documenti, di formazione del fascicolo digitale e di corretta gestione e formazione dell'archivio corrente e di deposito.

5.1 Titolario o piano di classificazione

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell’archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario), cioè di quello che si suole definire “sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell’analisi delle funzioni dell’ente, al quale viene ricondotta la molteplicità dei documenti gestiti”.
Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d’archivio in base alle funzioni e alle materie di competenza dell’ente.
Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell’ente, soggette a modifiche in forza di leggi o regolamenti.
Le modifiche al Titolario sono apportate con provvedimento esplicito della funzione di governo dell’Amministrazione.
La revisione anche parziale del Titolario viene proposta dal RSP quando necessaria ed opportuna.
Dopo ogni modifica del Titolario, il RSP provvede ad informare tutti i soggetti abilitati all’operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo delle nuove classifiche.
Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Viene garantita la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

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

5.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Essa è generalmente strutturata a livelli che si articolano gerarchicamente tra loro.
Le voci di primo e secondo livello del titolario (titoli e classi) individuano le funzioni primarie e di organizzazione dell'Ente.
L'elenco dei titoli e delle classi associate è disponibile nell'allegato 3.

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

Le operazioni di classificazione vengono generalmente svolte in momenti diversi e da personale differente.
I primi due livelli di classificazione (*titolo-classe*) vengono attribuiti nella fase di protocollazione; l'individuazione dei successivi livelli (*macro-fascicolo,* fascicolo, sotto-fascicolo digitale...) è invece generalmente demandata al Responsabile del procedimento o suo incaricato.
Tutti i documenti ricevuti e prodotti dall'Ente, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.

5.3 La fascicolazione

I documenti ricevuti e prodotti dall'Ente sono raccolti in fascicoli costituiti in modo che ciascuno rappresenti l'insieme ordinato dei documenti riferiti ad uno stesso procedimento amministrativo o, comunque, ad una stessa pratica.

I fascicoli possono essere:

- **Fascicoli cartacei**: laddove tutta la documentazione originale della pratica è prodotta in formato cartaceo;
- **Fascicoli informatici**: laddove tutta la documentazione originale della pratica è prodotta in formato elettronico;
- **Fascicoli ibridi**: nel caso in cui la documentazione riguardante la pratica sia stata formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico. In questi casi vengono prodotti due fascicoli distinti:
    - un fascicolo cartaceo nel quale viene raccolta la documentazione cartacea
    - un fascicolo informatico, archiviato nel sistema di gestione documentale, nel quale sono raccolti tutti i documenti prodotti in formato elettronico e i riferimenti di protocollo dei documenti prodotti in formato cartaceo.

  I due fascicoli sono collegati tra loro e i riferimenti al fascicolo collegato sono riportati sia nella copertina del fascicolo cartaceo che nei dati di identificazione del fascicolo informatico.

Oltre ai fascicoli informatici possono essere costituiti fascicoli per serie documentale, in cui vengono aggregati documenti della stessa tipologia.
I Responsabili degli singoli uffici interni dell'AOO forniscono le indicazioni operative per la gestione dei fascicoli e assicurano che la costituzione dei fascicoli avvenga secondo modalità uniformi, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco che di quelli adottati per la descrizione del fascicolo.

I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.

5.4 La fascicolazione digitale

Il fascicolo digitale corrisponde generalmente ad una "Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.
La formazione dei fascicoli tiene conto di come sia opportuno allocare le risorse umane addette alle pratiche in modo da razionalizzare l'impiego delle specifiche competenze degli appartenenti ai diversi settori di attività.
Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, il soggetto preposto provvede all'apertura di un nuovo fascicolo/sottofascicolo collegato ad un macro-fascicolo digitale già esistente.

La formazione di un nuovo fascicolo/sotto-fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali (metadati) cosi come previsto nell'allegato 5 del D.P.C.M del 3 dicembre 2013 (*regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005)*
L'insieme minimo dei metadati attribuiti ai fascicoli digitali è riportato nell'allegato 6 del presente manuale.

Ogni unità organizzativa è responsabile per la creazione e la gestione dei fascicoli nell'ambito dei servizi di competenza e delle prestazioni effettuate. I documenti contenuti in un fascicolo hanno di norma identica classificazione, e sono facilmente ricercabili sia attraverso quest'ultima che attraverso metadati.
I criteri di visibilità dei fascicoli digitali e dei loro relativi sottofascicoli all'interno dell'AOO sono definiti dai vari Responsabili dei Procedimenti Amministrativi in accordo con il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.
I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.
Si riporta di seguito la struttura di base del sistema di fascicolazione.

5.4.1 Processo di assegnazione dei fascicoli digitali ai documenti

Quando un nuovo documento viene recapitato al servizio competente o creato dall'Ente, il Responsabile del servizio o suo incaricato stabilisce se il documento si riferisce a un nuovo affare o procedimento; in caso affermativo è necessario aprire un nuovo fascicolo, altrimenti, se il documento stesso può essere ricollegato ad un affare o procedimento in corso, viene inserito in un fascicolo digitale già esistente.
A seconda delle ipotesi, si procede come segue:

- Se il documento dà avvio ad un *NUOVO PROCEDIMENTO*, il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo/sottofascicolo collegato al macro-fascicolo;
  - collega il documento al nuovo fascicolo aperto;
  - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà istruire la pratica.

- Se il documento si ricollega ad un *affare o procedimento in corso*,l'addetto:
  - seleziona il relativo fascicolo utente collegato al macro-fascicolo;
  - collega il documento al fascicolo selezionato;
  - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà gestire la pratica.

5.4.2 Modifica delle assegnazioni dei fascicoli digitali

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico.
Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora dell'operazione.

5.4.3 Chiusura dei fascicoli digitali

Il fascicolo digitale viene chiuso generalmente al termine del procedimento amministrativo o all'esaurimento dell'affare.

5.5 Serie archivistiche e repertori

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.
Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

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

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

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

L'Archivio è il complesso dei documenti prodotti o acquisiti dall'Ente durante lo svolgimento della propria attività.
I documenti amministrativi prodotti e detenuti da questo Ente sono oggetto di tutela ai sensi dell'art.10 del Codice dei beni culturali di cui al decreto legislativo 42/2004 pertanto tutti i soggetti che agiscono nell'ambito del sistema di gestione documentale del'Ente svolgono attività archivistica.
L'Ente, ai sensi dell'art. 30 del predetto Codice, assolve all'obbligo di conservazione e ordinamento degli archivi.
Ai fini di un corretto esercizio dell'azione amministrativa, i fascicoli prodotti dagli uffici dell'Ente sono raccolti in archivi che possono essere distinti in:

- ***archivio corrente***, la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione.
  L'archiviazione corrente si identifica per i documenti e i fascicoli informatici con l'archiviazione all'interno del sistema di gestione documentale
- ***archivio di deposito***, la parte di documentazione di affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso;
- **archivio storico**, la parte di documentazione relativa agli affari esauriti destinata alla conservazione perenne

La coesistenza, nell'ambito di uno stesso procedimento, di documenti di natura mista (digitali e cartacei) dà vita al cosiddetto "archivio ibrido".
Nel sistema documentale informatico basta chiudere un fascicolo per farlo passare all'archivio di deposito.
I fascicoli cartacei chiusi fanno parte dell'archivio di deposito tradizionale. Tutti i fascicoli cartacei chiusi, che non servono più per la consultazione, possono essere spostati anche fisicamente nell'archivio di deposito comunale.

La gestione dei processi di selezione dei documenti dell'archivio di deposito, può condurre a due esiti tra di loro contrastanti: la conservazione permanente dei documenti che rivestono significativo valore di testimonianza storica, oltre che rilevanza giuridico probatoria, oppure lo scarto, cioè l'eliminazione irreversibile dei documenti ritenuti di valore transitorio e strumentale, da effettuare con l'autorizzazione del soprintendente archivistico competente per territorio.

Secondo le diverse tipologie documentali gestite dall'Ente sono definiti criteri e regole di selezione al fine di individuare i documenti da scartare e quelli da conservare.

1) L'elenco delle tipologie di documenti soggetti a conservazione permanente sono:

a) i "verbali", ovvero documenti "contenenti la descrizione di un fatto" quali ad es. i verbali di seduta di Giunta o di Consiglio, ovvero i verbali di una seduta di gara. di una commissione di esami, etc;
b) Statuti, Regolamenti, Decreti, Ordinanze, Interpellanze, interrogazioni, mozioni,Verbali Nucleo di Valutazione, Provvedimenti dirigenziali, Registro di protocollo,Registro albo pretorio,Registro notifiche,Atti relativi a partecipazione societarie - Documentazione relativa alle elezioni amministrative, Atti e documenti del contenzioso legale,Schedari, rubriche e repertori dell'archivio,Atti relativi a riordinamenti e scarti archivistici
c) provvedimenti costitutivi, modificativi od estintivi di posizioni giuridiche e quindi anche determinazioni, concessioni, autorizzazioni, nulla osta etc;
d) documenti relativi all'attività contrattuale: Contratti - Verbali di gara - Bandi di gara - Offerta dell'impresa aggiudicataria - Capitolati di gara - Documentazione relativa alla qualificazione.
e) documenti prodotti da terzi ma con efficacia costitutiva di diritti soggettivi o abilitativi all'esercizio di attività quali ad esempio dichiarazioni di inizio attività (DIA), segnalazioni certificate di inizio attività (SCIA) etc;
f) i "registri", ovvero quei documenti "sui quali vengono annotati in sequenza, secondo criteri predefiniti (tendenzialmente cronologici), una pluralità di fatti o atti giuridici" (es. il registro delle notifiche, il registro del protocollo, il registro degli infortuni, il repertorio dei contratti);
g) tutti i documenti sottoscritti con firma digitale;
h) tutti i documenti inviati e ricevuti con posta elettronica certificata;
i) studi e relazioni tecniche, ricerche, pubblicazioni, documentazione fotografica, che siano propedeutici a piani, programmi e delibere di carattere generale.

2) Documenti da conservare 40 anni
   Mandati di pagamento e reversali di riscossione

3) Documenti da conservare per 15 anni
   Strumenti urbanistici e documenti correlati

4) Documenti da conservare per 10 anni
   a) i processi verbali relativi a sanzioni elevate nella materia di competenza dell'Ente (polizia amministrativa, commerciale, codice della strada, abusi edilizi); offerte delle ditte non aggiudicatarie, libri contabili etc;
   b) Concorsi (domande di partecipazione, elaborati scritti/pratici conservando eventualmente campionatura)- Gestione fiscale e assicurativa dei dipendenti e collaboratori (CUD,modello 730/4, denunce contributive annuali, autoliquidazione Inail, modelli di versamento ai fini contributivi previdenziali e fiscali, cedolini buste paga mensili, denuncia Statistiche sul personale
5) Documenti soggetti a conservazione per 5 anni sono:
   a) le richieste e la documentazione allegata, le pezze giustificative, i rendiconti relativi ai "contributi" ovvero le elargizioni di denaro - comunque denominate - erogate dall'Ente;
   b) la corrispondenza di carattere occasionale (le cosiddette "carte varie") ovvero "il complesso delle lettere e delle note scritte, inviate e ricevute dall'Ente" con riferimento ad un affare individuato ma che, per la loro scarsa importanza non siano sfociate in una delibera o provvedimento di altro genere, rimaste per così dire senza seguito;
   c) i certificati o le dichiarazioni attestanti qualità o stati personali con validità temporale limitata (art. 41 DPR 445);
   d) i dati statistici non relativi ad attività dell'Ente;
   e) la documentazione fiscale per la quale la legge prevede tale termine di conservazione;
   f) documenti relativi alla gestione ordinaria del personale.

5.6.1 Procedure di scarto

Per quanto riguarda le procedure di scarto dovrà farsi riferimento alle procedure previste dalla Sovrintendenze archivistica regionali.

In ogni caso si dovrà procedere a:
- Predisposizione della proposta di scarto indicando la documentazione che si intende scartare;
- Presentare di apposita istanza di autorizzazione alla Soprintendenza archivistica competente per territorio;
- Rilascio dell'autorizzazione da parte della Soprintendenza con approvazione dell'elenco di scaro con apposito provvedimento
- Distruzione della documentazione scartata con verbalizzazione delle operazioni.

6 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Il presente capitolo illustra le modalità di produzione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

6.1 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. 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 sul protocollo viene considerata giuridicamente inesistente presso l’amministrazione. Non è consentita la protocollazione di un documento già protocollato. Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.
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.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l’immodificabilità del contenuto

6.2 Registrazione di protocollo

Di seguito vengono illustrate le regole 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;
- l’indicazione del mittente o del destinatario, registrata in forma non modificabile;
- l’oggetto del documento, registrato in forma non modificabile;
- la data e protocollo del documento ricevuto, se disponibili;
- la classificazione;
- l’impronta del documento informatico.

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

6.3 Elementi facoltativi delle registrazioni di protocollo

Il Responsabile del Servizio Protocollo, con proprio provvedimento e al fine di migliorare la gestione, la ricerca e la conservazione della documentazione, può modificare e integrare gli elementi facoltativi del protocollo, anche per singole categorie o tipologie di documenti.
La registrazione degli elementi facoltativi del protocollo, previa autorizzazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico, può essere modificata, integrata e cancellata in base alle effettive esigenze delle unità organizzative o del servizio protocollo. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

6.4 Segnatura di protocollo dei documenti

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

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.
Le informazioni previste sono:

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

Per i documenti analogici le informazioni sopra riportate vengono riportate sul documento attraverso il timbro di registratura di protocollo.
Per i documenti informatici tutte le informazioni sopra riportate sono generate automaticamente dal sistema e sono incluse nella segnatura informatica di ciascun messaggio protocollato

6.5 Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori e immodificabili della registrazione di protocollo per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare la 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, insieme a data, ora e autore dell'annullamento e agli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.
In tale ipotesi la procedura riporta l'annotazione di annullamento. Il sistema inoltre registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.
Solo il Responsabile della gestione documentale e del Servizio di Protocollo informatico è autorizzato ad annullare, direttamente o delegando gli addetti, una registrazione di protocollo.
L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile della gestione documentale e del Servizio di Protocollo informatico.

6.6 Protocollazione documenti interni formali

I documenti formali prodotti e scambiati internamente sono soggetti a protocollazione e indicati come protocolli interni. Vengono inseriti nel sistema di gestione documentale con opportuna classificazione, assegnazione di visibilità, collegamento ai documenti o procedimenti correlati, fascicolazione e archiviazione.

6.7 Oggetti ricorrenti

Ciascun Servizio può individuare tipologie di documenti per i quali concordare con il Protocollo generale l'indicazione esatta dell'oggetto, la titolazione, la tipologia e l'assegnazione a predeterminati soggetti o ambiti organizzativi.
E' compito di ciascun Servizio provvedere a verificare il permanere dell'attualità di ciascun oggetto individuato e del relativo smistamento.

6.8 Registrazione differita di protocollo

Per "protocollo differito" si intende la registrazione di documento in arrivo che indica nello specifico la data alla quale si riferisce il ricevimento del documento stesso e la causa che ne ha determinato il differimento.
E' possibile effettuare la registrazione differita di protocollo, qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi.
La registrazione differita di un documento in arrivo nel sistema va richiesta e deve essere autorizzata dal Responsabile della gestione documentale e del Servizio di Protocollo informatico o suo delegato.

6.9 Documenti riservati (Protocollo riservato)

Sono previste particolari forme di riservatezza per i documenti relativi a procedimenti disciplinari nei confronti dei dipendenti, vicende o a fatti privati, politici o giudiziari (giudizi pendenti) o documenti che richiedono, comunque, una trattazione riservata. Per tali atti sul registro di protocollo generale compare solo il numero attribuito a ciascun documento e l'annotazione “Riservato”.
I documenti registrati con tali forme appartengono al cosiddetto “protocollo riservato” costituito dalle registrazioni il cui accesso è autorizzato solo alle persone espressamente abilitate. Queste ultime hanno comunque la visibilità dei soli documenti riservati trattati dall’unità di appartenenza. Le procedure adottate per la gestione dei documenti ad accesso riservato, comprese le registrazioni, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti.

7 IL SISTEMA DI GESTIONE DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

Il sistema di gestione documentale e di protocollazione adottato dall’Ente è basato sulla piattaforma della soluzione software **OLIMPO – archiviazione documentale e scrivania digitale della SISCOM spa**. La soluzione per la protocollazione prevede un modulo specifico denominato Egisto che gestisce tutte le fasi di protocollazione in arrivo/partenza nonche’ di protocolli interni in modo totalmente integrato con il sistema documentale..
La soluzione gestisce la ricezione e trasmissione delle pec e mail con la protocollazione e l’archiviazione nel sistema documentale in modo sicuro e non modificabile. I documenti pervenuti vengono condivisi agli uffici ed operatori destinatari e vengono tracciati nell’iter burocratico.

I documenti prodotti dall’Ente vengono gestiti nell’ambito del sistema documentale sia nella fase di redazione che in quella di archiviazione, di protocollazione e di trasmissione. Il tutto il modo integrato.

7.1 Descrizione funzionale ed operativa

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico, gestione documentale e dei procedimenti adottato dall'Ente, con particolare riferimento alle modalità di utilizzo dello stesso.

La descrizione funzionale ed operativa del sistema di protocollo informatico vengono specificate in dettaglio all'interno dell'allegato 7.

8 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione può riguardare sia documenti informatici all'origine che documenti analogici convertiti in formato digitale.

8.1 Principi sulla conservazione dei documenti informatici

La conservazione digitale è l'insieme delle attività e dei processi che, tramite l'adozione di regole, procedure e tecnologie, garantiscono l'accessibilità, l'utilizzabilità (leggibilità e intelligibilità), l'autenticità (identificabilità univoca e integrità) e la reperibilità dei documenti e dei fascicoli informatici con i metadati ad essi associati nel medio e nel lungo periodo, in un ambiente tecnologico presumibilmente diverso da quello originario.
Il valore legale dell'attività di conservazione è subordinato all'organizzazione del servizio e allo svolgimento dell'attività secondo le regole tecniche vigenti.
Il sistema di conservazione opera trattando dei Pacchetti informativi, contenitori che racchiudono uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche) o anche i soli metadati riferiti agli oggetti da conservare.

I pacchetti informativi possono avere varia natura:

- di versamento: pacchetto inviato dal produttore del documento al sistema di conservazione secondo il formato predefinito e concordato, descritto nel manuale di conservazione.
  Con il versamento effettuato dal responsabile della gestione documentale o del protocollo il documento, il fascicolo informatico o l'aggregazione transitano dal sistema di gestione documentale al sistema di conservazione.
- di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento utilizzando le specifiche contenute nell'allegato 4 del D.P.C.M e secondo le modalità riportate nel manuale di conservazione.
- di distribuzione: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta

Il processo di conservazione si articola nelle seguenti fasi:

1) acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;

2) verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato all'art. 11 del D.P.C.M;
NB: nel caso in cui la verifica evidenzi anomalie il pacchetto di versamento viene rifiutato;

3) trasmissione del pacchetto di versamento in modalità sicura;

4) preparazione, sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del D.P.C.M. e secondo le modalità riportate nel manuale della conservazione;

5) preparazione e la sottoscrizione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

6) ai fini della interoperabilità tra sistemi di conservazione, produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;

7) produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;

8) produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11 del D.P.C.M., in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;

9) scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore;

8.2 La conservazione dei documenti informatici dell'Ente

L'Ente decide di affidare la gestione della conservazione ad outsourcer esterno accreditato.

Il "ciclo di gestione della conservazione" ed il servizio adottato dall'Ente vengono descritti in dettaglio nell'allegato 8.

9 REGISTRO DI EMERGENZA

9.1 Utilizzo del registro di emergenza

Il responsabile del servizio di protocollo informatico autorizza lo svolgimento delle operazioni di registrazione di protocollo sull'apposito registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.
Il registro di emergenza è unico ed è gestito dall'Ufficio Protocollo. Tutti i servizi comunali, in caso di necessità, fanno quindi riferimento a questo ufficio per ottenere l'assegnazione di un numero di protocollo di emergenza, in entrata o in uscita.
Il registro di emergenza si rinnova ogni anno solare, pertanto inizia il primo gennaio e termina il 31 dicembre di ogni anno.
Si applicano le seguenti modalità di registrazione e di recupero dei dati:

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

10 SICUREZZA

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dall'applicazione informatica adottata dall'Ente.
Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.
Il presente capitolo riporta le misure di sicurezza adottate specifiche per l'infrastruttura di protocollo informatico anche in relazione alle norme sulla protezione dei dati personali.

10.1 Obiettivi

La politica in merito alla sicurezza di questo Ente è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

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

10.2 Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite.
Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.
Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l'identificazione dell'utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal responsabile della pratica o del procedimento.
L'accesso diretto alla banca dati, l'inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema.
I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.
Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.
Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all'accesso, garantendo comunque il diritto alla riservatezza e all'oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.
Gli accessi esterni vengono di norma gestiti attraverso il sito web dell'Ente. I dati in libera consultazione vengono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consentano il riutilizzo.

10.3 Sicurezza nella 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 con AOO diverse.

I documenti sono prodotti con l'ausilio dell'applicativo specificato nell'allegato 7 che possiede i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF/A, XML, TIFF.
I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF/A, 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.
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.

10.4 Trasmissione ed 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, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

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

10.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso 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.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso 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.

11 NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il "Manuale di gestione" su proposta del responsabile del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (RSP).
Il Manuale sarà aggiornato a seguito di:
• normativa sopravvenuta;

• introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
• inadeguatezza delle procedure rilevata nello svolgimento delle attività correnti;
• introduzione di nuove procedure
Il Manuale viene approvato e modificato con deliberazione della Giunta.
Gli allegati sono modificati, di norma e fatte salve le eccezioni esplicitamente dichiarate, con provvedimenti del Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

11.2 Pubblicità del manuale

Il Manuale, a norma dell'art. art.15 della legge n. 15 del 2005, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.
Inoltre copia del presente Manuale è:
• resa disponibile a tutto il personale dell'AOO tramite il sistema di gestione documentale;
• inviata all'organo di revisione;
• pubblicata sul sito internet dell'Amministrazione.

11.3 Entrata in vigore

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

COMUNE DI GRIGNASCO

ALLEGATO 1

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Norme di riferimento

1. D.P.R. n. 513 del 10 novembre 1997
2. D.P.R. n. 445 del 28 dicembre 2000
3. Deliberazione AIPA n. 42 del 2001
4. Decreto Legislativo 23 gennaio 2002, n. 10
5. Decreto del Presidente della Repubblica 07 aprile 2003, n. 137
6. D.P.C.M. del 13 gennaio 2004
7. Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004
8. D.P.R. del 11 febbraio 2005
9. Decreto legislativo 07 marzo 2005 n. 82 – Codice dell'amministrazione digitale
10. D.P.C.M. del 30 marzo 2009
11. Deliberazione CNIPA 21 maggio 2009, n. 45
12. Decreto Legge n. 5 del 09 febbraio 2012
13. D.P.C.M. del 22 febbraio 2013 pubblicato in GU n. 117 del 21-05-2013
14. D.P.C.M. del 21 marzo 2013 pubblicato in GU n. 131 del 06-06-2013
15. Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi dell'artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui D.L. 82/2005
16. Circolare AgID n. 65 del 10 aprile 2014 pubblicata in GU n. 89 del 16 aprile 2014
17. D.P.C.M. 14 novembre 2014

COMUNE DI GRIGNASCO

ALLEGATO 2

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO PER LA

COMUNE DI GRIGNASCO

Provincia di Novara

Prot. N. 7814 Grignasco 08.10.2015

Decreto n. 06/2015

OGGETTO: NOMINA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE

IL SINDACO

PREMESSO che il Comune di Grignasco si articola in un'unica Area Organizzativa Omogenea;

ATTESO che in attuazione del Codice dell'Amministrazione Digitale recato dal D. Lgs. 82/2005 nel testo vigente, delle Regole Tecniche sul protocollo approvate con D.P.C.M. 3 dicembre 2013 e delle Regole Tecniche sulla conservazione documentale approvate con D.P.C.M. 3 dicembre 2013 si rende necessario provvedere ad individuare il Responsabile della gestione documentale ed il Responsabile della conservazione per l'unica area organizzativa omogenea;

DATO ATTO che al Responsabile della gestione documentale sono demandate, ai sensi degli articoli 4 e seguenti delle precitate regole tecniche, le seguenti incombenze**:**

a) La predisposizione dello schema del manuale di gestione previsto dall'art. 5 delle regole tecniche.
b) La predisposizione del piano per la sicurezza informatica relativo a tutto il flusso documentale con riferimento alle misure minime di sicurezza previste dal codice per la protezione dei dati personali recato del decreto legislativo 30 giugno 2003, n. 196. Tale attività devono essere svolta in collaborazione ed intesa con gli altri soggetti individuati dalle regole tecniche e quindi il responsabile della conservazione, il responsabile dei sistemi informativi, il responsabile del trattamento dei dati personali.
c) La definizione e l'applicazione di criteri uniformi di trattamento del documento informatico con particolare riguardo a:

- classificazione
- archiviazione.

d) La formazione del pacchetto di versamento e quindi del transito del documento del sistema di conservazione.

CONSIDERATO che, in relazione al ruolo centrale del responsabile della gestione documentale nell'organizzazione del sistema di gestione documentale e della successiva

responsabilità in ordine alla concreta attuazione del manuale di gestione documentale, occorre che il responsabile in argomento sia in possesso di competenza:

- di natura giuridica, considerando che il manuale di gestione documentale ha comunque natura regolamentare;
- conoscenza dell'organizzazione dell'Ente e delle eventuali criticità per quanto attiene le

risorse umane e strumentali;

- capacità di condivisione delle scelte con gli altri soggetti coinvolti nell'organizzazione della

gestione documentale.

Ritenuto che il responsabile della gestione documentale debba essere individuato all'interno dell'Ente a livello apicale, potendo eventualmente avvalersi, per quanto concerne gli aspetti eminentemente tecnico informatici, di un supporto esterno;

Ritenuto pertanto di nominare quale Responsabile della gestione documentale di questo il Dott. Michele REGIS MILANO

Rilevato che la normativa sopra richiamata dispone l'obbligo di individuare, al fine di garantire la continuità dello svolgimento delle funzioni rimesse al Responsabile della gestione documentale, un vicario;

Ritenuto di individuare il vicario del Responsabile della gestione documentale l' amministrativo dell'Ente signora Valentina Bonazzi inquadrato nella categoria D;

Ritenuto di individuare il vicario del Responsabile della gestione documentale l' amministrativo dell'Ente signor Marco Garino inquadrato nella categoria B;

Ritenuto opportuno individuare nel responsabile della gestione documentale il responsabile della conservazione documentale, così pure come nei vicari, i vicari per la conservazione;

Dato atto che il Responsabile della gestione documentale e della conservazione non dispone di autonomo potere di spesa né di assegnazione di risorse del bilancio dell'Ente e che la presente nomina non dà luogo alla percezione di compensi accessori;

Visto lo Statuto Comunale vigente;

Visti e richiamati

- il Decreto Legislativo 82/2005 recante il codice dell'Amministrazione Digitale

- i DD.PP.CC.MM in data 3 dicembre 2013 recanti le regole tecniche per il protocollo e la conservazione documentale;

Visto il TUEL recato dal decreto legislativo 267/2000;

DECRETA

DI NOMINARE quale Responsabile della gestione documentale e Responsabile della conservazione di questo Comune, articolato in unica Area Omogenea, il dott. Michele REGIS MILANO al quale sono demandate le competenze e gli adempimenti previsti dalle Regole Tecniche per il protocollo e per la conservazione documentale;

DI NOMINARE quale Responsabile della gestione documentale e Responsabile della conservazione vicario il signor Valentina Bonazzi e il sig. Marco Garino, dipendenti di questo Comune, inquadrati, rispettivamente, nella categoria D e B;

DI DARE ATTO che il Responsabile della gestione documentale e della conservazione ed il vicario non dispongono di autonomo potere di spesa né di assegnazione di risorse del bilancio dell'Ente e che la presente nomina non dà luogo alla percezione di compensi accessori;

Il Sindaco

Sottoscritto digitalmente ai sensi del D.Lgs 82/2005

Per accettazione

Sottoscritto digitalmente ai sensi del D.Lgs 82/2005

Sottoscritto digitalmente ai sensi del D.Lgs 82/2005

COMUNE DI GRIGNASCO

ALLEGATO 4

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

I FORMATI DEI DOCUMENTI

TITOLI E CLASSI

I FORMATI DEI DOCUMENTI

(Estratto dell'allegato 2 al D.P.C.M 3 dicembre 2013)

Indice

[…]

1 INTRODUZIONE

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

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

2 I FORMATI

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.

2.1 Identificazione

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

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

2.2 Le tipologie di formato

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

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

- Testi/documenti (DOC, HTML, PDF,...)
- Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)

- Suoni (MP3, WAV, ...)
- Video (MPG, MPEG, AVI, WMV,...)
- Eseguibili (EXE, ...)
- Archiviazione e Compressione (ZIP, RAR, ...)
- Formati email (SMTP/MIME, …)

2.3 Formati Immagini

Per la rappresentazione delle immagini sono disponibili diversi formati, che possono essere distinti secondo la grafica utilizzata: raster o vettoriale.

2.3.1 Raster

Nel caso della grafica raster, l'immagine digitale è formata da un insieme di piccole aree uguali (pixel), ordinate secondo linee e colonne.

I formati più diffusi sono il .tif (usato dai fax), il .jpg, il .bmp.

2.3.2 Vettoriale

La grafica vettoriale è una tecnica utilizzata per descrivere un'immagine mediante un insieme di primitive geometriche che definiscono punti, linee, curve e poligoni ai quali possono essere attribuiti colori e anche sfumature.

I documenti realizzati attraverso la grafica vettoriale sono quelli utilizzati nella stesura degli elaborati tecnici, ad esempio progetti di edifici.

Attualmente i formati maggiormente in uso sono:

x DWG, un formato proprietario per i file di tipo CAD, di cui non sono state rilasciate le specifiche;

x DXF, un formato simile al DWG, di cui sono state rilasciate le specifiche tecniche x Shapefile un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con con i prodotti che usano i precedenti formati.

x SVG, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

2.4 Altri Formati

Per determinate tipologie di documenti informatici sono utilizzati specifici formati. In particolare in campo sanitario i formati più usati sono:

x DICOM (immagini che arrivano da strumenti diagnostici) anche se il DICOM non è solo un formato, ma definisce anche protocolli e altro;

x HL7 ed in particolare il CDA2 (Clinical Document Architecture) che contiene la sua stessa descrizione o rappresentazione.

[..]

2.5 Le caratteristiche generali dei formati

L'informazione digitale è facilmente memorizzata, altrettanto facilmente accedere e riutilizzarla, modificarla e manipolarla, in altre parole, elaborarla ed ottenere nuova informazione.

Questi formati, e i programmi che li gestiscono, che sono poi quelli che consentono e facilitano l'operatività giorno per giorno sul digitale, vanno valutati in funzione di alcune caratteristiche quali:

La diffusione, ossia il numero di persone ed organizzazioni che li adotta

La portabilità, ancor meglio se essa è indotta dall'impiego fedele di standard documentati e accessibili

Le funzionalità che l'utente ha a disposizione per elaborare l'informazione e collegarla ad altre (ad esempio gestione di link)

La capacità di gestire contemporaneamente un numero congruo (in funzione delle esigenze dell'utente) di formati

La diffusione di visualizzatori che consentono una fruibilità delle informazioni in essi contenute indipendentemente dalla possibilità di rielaborarle.

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.

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

3 CRITERI DI SCELTA DEI FORMATI

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

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

3.1 Caratteristiche

Le caratteristiche di cui bisogna tener conto nella scelta sono:

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

3.1.1 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.

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

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

3.1.2 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

3.1.3 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.

3.1.4 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.

3.1.5 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.).

3.1.6 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.

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 SCELTA

4.1 Formati e prodotti per la formazione e gestione

Per la scelta dei formati idonei alla formazione e gestione dei documenti informatici, sono da tenere in considerazione le caratteristiche indicate nei paragrafi precedenti. Ulteriori elementi da valutare sono l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento. Le pubbliche amministrazioni indicano nel manuale di gestione i formati adottati per le diverse tipologie di documenti informatici motivandone le scelte effettuate; **specificano altresì i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.**

4.2 Formati per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche. Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti informatici. Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici. I formati per la conservazione adottati per le diverse tipologie di documenti informatici devono essere indicati nel manuale di conservazione motivandone le scelte effettuate; sono altresì specificati i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.

[...]

COMUNE DI GRIGNASCO

ALLEGATO 5

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

METADATI MINIMI DEL DOCUMENTO INFORMATICO

METADATI MINIMI DEL DOCUMENTO INFORMATICO

Il presente allegato illustra la struttura dei metadati relativi al documento informatico e al documento amministrativo informatico.

Metadati minimi del documento informatico

```
<?xmlversion="1.0"encoding="ISO-8859-1"?>
<xs:schemaxmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:elementname="documento">
<xs:complexType>
<xs:sequence>
<xs:elementname="datachiusura"type="xs:date"/>
<xs:elementname="oggettodocumento"type="xs:string/>
<xs:elementname="soggettoproduttore">
<xs:complexType>
<xs:sequence>
<xs:elementname="nome"type="xs:string"/>
<xs:elementname="cognome"type="xs:string"/>
<xs:elementname="codicefiscale"type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:elementname="destinatario">
<xs:complexType>
<xs:sequence>
<xs:elementname="nome"type="xs:string"/>
<xs:elementname="cognome"type="xs:string"/>
<xs:elementname="codicefiscale"type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
```

```
</xs:sequence>
<xs:attributename="IDDocumento"type="xs:string"use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

Informazione	Valori Ammessi	Tipodato	xsd
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri	<xs:attribute name="IDDocumento" type="xs:string" use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)			

Informazione	Valori Ammessi	Tipodato	xsd
Datadichiusura	Data	Data formato gg/mm/aaaa	<xs:element name="datachiusura" type="xs:date"/>
Definizione			
Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile			

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

Informazione	Valori Ammessi	Tipodato	xsd
Soggetto produttore	Nome: testo libero	Alfanumerico 40 caratteri	<xs:element name="soggettoproduttore"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	Cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: Codice Fiscale	Alfanumerico 16 Caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a produrre il documento informatico.			

Informazione	Valori Ammessi	Tipodato	xsd
Destinatario	Nome: testo libero	Alfanumerico 40 caratteri	<xs:element name="destinatario"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale"
	Cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale:	Alfanumerico 16	

	Codice Fiscale **(Obbligatorio, se disponibile)**	Caratteri	type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
Definizione			
Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico.			

Metadati minimi del documento amministrativo informatico

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

COMUNE DI GRIGNASCO

ALLEGATO 6

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

METADATI MINIMI DEL FASCICOLO INFORMATICO O DELLA

METADATI MINIMI DEL FASCICOLO INFORMATICO O DELLA AGGREGAZIONE DOCUMENTALE INFORMATICA

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

Informazione	**Valori Ammessi**	**Tipodato**	**xsd**
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri	<xs:attribute name="IDFascicolo" type="xs:string" use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al			

fascicolo o aggregazione documentale informatica in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)

Informazione	Valori Ammessi	Tipodato	xsd
Amministrazione titolare	Vedi specifiche Codice IPA	Codice IPA	<xs:element name="IPAtitolare" type="xs:string maxOccurs="1"/>
Definizione			
Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo.			

Informazione	Valori Ammessi	Tipodato	xsd
Amministrazioni partecipanti	Vedi specifiche Codice IPA	Codice IPA	<xs:element name="IPApartecipante" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
Definizione			
Amministrazioni che partecipano all'iter del procedimento.			

Informazione	Valori Ammessi	Tipodato	xsd
Responsabile del procedimento	Nome: testo libero	Alfanumerico 40 caratteri	<xs:element name="responsabile"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	Cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri	
Definizione			
Responsabile del procedimento			

Informazione	Valori Ammessi	Tipodato	xsd
Oggetto	Testo libero	Alfanumerico 100 caratteri	<xs:element name="oggettofascicolo" type="xs:string />

Definizione
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublic Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.

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

COMUNE DI GRIGNASCO

ALLEGATO 7

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

IL SISTEMA DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

INDICE

1. Premessa: Il sistema documentale e di protocollazione adottato dall'Ente

L'Ente ha adottato e sta operando con la piattaforma di gestione documentale denominata **"OLIMPO"** che ha un modulo specifico per la protocollazione denominato "EGISTO".
La soluzione riunisce tutte le funzionalità necessarie per gestire la documentazione ed i procedimenti amministrativi informatici relazionandosi con gli altri applicativi gestionali e integrando i servizi di protocollo Informatico, gestione Elettronica Documentale, scrivania digitale, archiviazione digitale, fascicolazione, gestione dei Procedimenti Amministrativi (Workflow), interscambio con il sito web per il Cittadino e conservazione.
Il sistema permette la gestione di documenti indipendentemente dal loro formato nativo (informatico all'origine o cartaceo digitalizzato).
Tutti i documenti informatici, sia creati dall'AOO che ricevuti dall'esterno sono archiviati automaticamente dal sistema di gestione documentale, contestualmente alle operazioni di registrazione e segnatura di protocollo, in un repository che ne garantisce la sicurezza e l'immodificabilità.
L'archivio è accessibile ai solo operatori accreditati e la ricerca è garantita da un sistema di reperimento parametrico dei documenti.
La piattaforma permette la protocollazione e l'archiviazione digitale di tutta la corrispondenza in arrivo dell'Ente e gestisce, in modo totalmente digitale, la distribuzione della posta agli uffici.
L'operazione di smistamento digitale è supportata da un'apposita area di monitoraggio denominata "*Quaderno di lavoro*", all'interno della quale ogni operatore è in grado di visionare la corrispondenza in arrivo, prenderla in carico, fascicolarla, assegnarla ed evaderla.
La corrispondenza in partenza viene gestita direttamente dalle unità organizzative che producono i documenti.
I documenti informatici possono essere creati direttamente dalla scrivania digitale o essere prodotti dagli applicativi gestionali integrati alla piattaforma di gestione documentale
Le operazioni di firma digitale, condivisione interna, protocollatura e segnatura, archiviazione, trasmissione e conservazione sono tutte integrate all'interno della piattaforma e sono riportate in evidenza all'operatore competente nell' area di monitoraggio sopra citata denominata "*Quaderno di lavoro*".
Inoltre, grazie al calendario digitale integrato, ogni appuntamento, scadenze o attività lavorativa può essere registrata dall'utente e mantenuta in evidenza nell'area di monitoraggio.
Il "*Quaderno di lavoro*" supporta così passo a passo l'operatore nell'espletamento di tutte le sue incombenze.

2. Gestione accessi

Il sistema OLIMPO gestisce un sistema di profilazione degli utenti e dei relativi diritti di accesso. Tutte le operazioni che si possono svolgere all'interno della procedura sono predeterminate: ogni singolo utente può avere il "diritto" o meno di svolgerle. In tal modo tutto ciò che accade nel sistema è controllato dal sistema stesso. Le azioni di ciascun utente vengono continuamente monitorate e registrate in automatico in appositi file di LOG, immodificabili.
A ciascun addetto vengono attribuiti un nome utente e una password, dei quali sarà unico responsabile sin dal momento della formale attribuzione. Con il primo accesso al sistema, l'utente è tenuto a modificare la password personale, individuandone un'altra nel rispetto dei parametri formali prestabiliti. Il sistema è configurato in modo tale che la password, da questo momento in avanti, non possa essere conosciuta da nessuno, nemmeno dall'amministratore di sistema.
Sono ammesse soltanto password conformi alla vigente normativa in materia di protezione, sicurezza e tutela dei dati personali. E' prevista la sostituzione periodica della password di accesso, in conformità alle disposizioni vigenti.

3. Inserimento/Formazione di un nuovo documento

L'inserimento di un documento è la prima operazione con la quale si confrontano quotidianamente gli operatori.
Esistono diverse modalità per inserire un nuovo documento in OLIMPO; di seguito verranno richiamate le principali.

Per formare un documento si parte dalla specifica funzione "NUOVO DOCUMENTO" e si redige il documento previa compilazione della maschera di indicizzazione.
La maschera di indicizzazione contiene le informazioni principali relative al documento, essenziali per la ricerca. Al fine di standardizzare il più possibile le metodologie di archiviazione dei documenti sono stati previsti campi con liste predefinite, utili nel prevenire errori di digitazione o impostazioni personali.

Il secondo modo di inserire un documento in OLIMPO è quello di partire da un documento simile già presente all'interno del sistema. In questo caso, dopo aver ricercato il documento di base, si procede duplicando la scheda relativa con il menù contestuale.
In alternativa, si può partire da un modello di documento già presente in OLIMPO . E' stato infatti predisposto sul sistema un tipo di documento denominato "*MODELLI*", con maschera di indicizzazione semplificata che permette di memorizzare agevolmente i modelli dei documenti più usati, ottimizzandone l'utilizzo ed evitando le fasi ripetitive.

E' inoltre possibile inserire in OLIMPO un documento, acquisendolo direttamente dal file system. Questo metodo è particolarmente indicato per tipologie di file provenienti da applicazioni che non dispongono di "macro" di inserimento.

I documenti provenienti dall'esterno vengono importati nel sistema in modo diretto se già in formato digitale, oppure vengono importati previa digitalizzazione tramite scansione.
I documenti informatici arrivati tramite posta elettronica sono gestiti automaticamente con apposita funzione. Se si tratta di messaggi di posta elettronica certificata inviati ad una delle caselle PEC comunali, sono gestiti dalla voce "PEC in arrivo".

4. Fascicolazione di un documento

L'operazione di fascicolazione è particolarmente importante per la ricerca sistematica dei documenti ed è prevista dalle regole tecniche del CAD. La classificazione dell'Ente viene riportata in dettaglio all'interno del capitolo *"4. Sistema di classificazione, fascicolazione digitale e archiviazione"* del manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi

OLIMPO prevede una funzionalità specifica per la gestione dei fascicoli digitali. La struttura dei fascicoli digitali di OLIMPO è correlata ai procedimenti gestiti dalle procedure gestionali e dalle procedure del sistema di workflow. Pertanto i fascicoli vengono alimentati da:

1. Documenti prodotti dall'Ente:
   - da sistema documentale
   - da procedure gestionali
   - da procedure workflow

2. Documenti pervenuti all'Ente

Quando viene prodotto un nuovo documento tramite specifica procedura gestionale del sistema integrato sarà la stessa a collocare il documento all'interno del relativo fascicolo digitale (macrofascicolo) ed a creare il fascicolo/sottofascicolo relativo all'affare o al procedimento in corso. Se esiste già il relativo sotto-fascicolo, il documento verrà automaticamente collegato ad esso.
Se il documento è prodotto invece tramite la scrivania digitale del sistema documentale OLIMPO, l'assegnazione del fascicolo e del relativo sotto-fascicolo sarà automatica se si risponde ad un documento già fascicolato, a carico del soggetto competente negli altri casi.

Per quanto riguarda invece i documenti pervenuti all'Ente, l'assegnazione del fascicolo e del relativo sotto-fascicolo è a carico del soggetto competente.

5. Ricerca dei documenti in archivio

OLIMPO possiede un efficiente sistema di ricerca e reperimento dei documenti basato sui dati inseriti nelle maschere di indicizzazione, al momento della memorizzazione del documento o anche in momenti successivi per i soli dati facoltativi. La ricerca di documenti può essere effettuata per documento singolo, per procedimento o per fascicolo, o in base ad altri criteri di individuazione (es. tipologia, classificazione ecc.). Il sistema di gestione documentale consente l'inserimento di modelli di ricerca e di consultazione, con maschere personalizzate, richiamabili ripetutamente nel tempo. La ricerca delle informazioni sul sistema è effettuata secondo criteri basati su tutti i tipi di informazione registrati. I criteri di selezione possono essere costituiti da espressioni semplici o da combinazioni di espressioni legate per mezzo di operatori logici. La ricerca può essere effettuata su singoli campi, o su parti del contenuto dei campi stessi.

6. Condivisione dei documenti

Tramite il sistema documentale è possibile condividere/inviare internamente un documento ad altri operatori con la specifica delle operazioni da compiere sul documento (consultazione, correzione, apposizione di firma digitale, protocollazione, invio all'esterno ecc..);

La peculiarità della posta OLIMPO, a differenza della posta elettronica tradizionale, consiste nel fatto che i documenti memorizzati nel sistema non vengono effettivamente inviati: ciò che viene trasmesso attraverso la posta è un link al documento, che è sempre unico all'interno del sistema, e come tale si presenta sempre aggiornato agli utenti che vi accedono. Il sistema consente di assegnare le visibilità, e di spedire i documenti con o senza "notifica" di avviso.
La ricezione di un documento condiviso viene segnalata su apposito nodo del quaderno di lavoro di OLIMPO accompagnata dalla specifica dell'operazione da compiere sul documento.

Grazie a questo sistema di condivisione/assegnazione interno non vi alcuna replicazione del documento.

7. Assegnazione dei documenti

Tramite il sistema documentale è possibile assegnare un documento ad uno o più "incaricati del procedimento/collaboratori".
Il documento assegnato viene ricevuto in apposito nodo del loro quaderno di lavoro di OLIMPO.
L'assegnazione può inoltre essere accompagnata da una nota operativa con la quale si possono indicare le eventuali modalità operative da eseguire.
L'assegnatario può monitorare in qualsiasi momento lo stato di avanzamento delle operazioni sul documento.

La peculiarità dell'assegnazione di OLIMPO, a differenza della posta elettronica tradizionale, consiste nel fatto che i documenti che vengono assegnati nel sistema non vengono effettivamente inviati: ciò che viene trasmesso è un link al documento, che è sempre unico all'interno del sistema, e come tale si presenta sempre aggiornato agli utenti che vi accedono.

8. Sottoscrizione documenti informatici

La firma digitale è strettamente connessa alla gestione documentale in quanto permette il passaggio definitivo dal formato cartaceo dei documenti, al formato digitale e alla conseguente eliminazione degli archivi cartacei. Questo strumento, tuttora sottoutilizzato rispetto alle sue potenzialità, rappresenta un prerequisito ineludibile per l'evoluzione della documentazione, sempre più destinata a trasformarsi da foglio di carta a file memorizzato nel sistema.
OLIMPO gestisce sia l'inserimento di documenti già firmati digitalmente, sia la firma diretta dei documenti all'interno del sistema.
Nei casi consentiti dalla legge, la firma digitale è sostituita da altre forme di firma elettronica o firma elettronica avanzata contemplate dal CAD e dalle regole tecniche vigenti.

9. Invio di un documento a destinatari esterni

E' possibile protocollare in uscita sia un documento già presente nell'archivio interno (duplicando la relativa scheda che di norma riporta anche la tipologia documentale appropriata), sia un documento in corso di inserimento nel sistema. Dopo avere compilato gli indici, il documento sarà opportunamente fascicolato e archiviato.

10. Iter documento

Tutte le azioni effettuate su un documento all'interno del sistema documentale (visualizzazione, lettura, presa in carico, assegnazione, ecc) vengono memorizzate automaticamente sul documento stesso in una specifica sezione di riepilogo delle operazioni effettuate; in questo modo è possibile monitorare, in qualunque momento, lo stato di avanzamento lavori del documento in esame.

11. Operatività del flusso dei documenti ricevuti dall'AOO

Una delle prime operazioni effettuate su documenti ricevuti è quella di procedere alla protocollazione della documentazione tramite il modulo software EGISTO.

EGISTO permette infatti di protocollare:

- E-mail Certificate/E-mail: il sistema protocolla automaticamente tutte le informazioni contenute nel messaggio di posta selezionato (*oggetto, mittente, allegati, riferimenti del protocollo ricevuto, ecc*);
- Istanze pervenute tramite apposito servizio on line dal sito dell'Ente: il sistema il sistema protocolla automaticamente tutte le informazioni ricevute;
- File informatici da supporti digitali esterni (*CD-ROM, DVD, hard disk, pen drive ecc.*)
- Documentazione cartacea (*posta ordinaria, raccomandata o consegnata a mano*) allegando la scansione della documentazione

Ultimata la protocollazione di un documento pervenuto, esso è reso immediatamente disponibile ai componenti delle varie unità organizzative competenti tramite il sistema di Gestione documentale "OLIMPO" all'interno dell'area di monitoraggio denominata "Quaderno di lavoro".
Le operazioni che possono essere effettuate sul documento ricevuto sono le seguenti:

- **Presa visione e mantenimento del documento sul quaderno di lavoro**
  Il documento pervenuto può essere visionato e mantenuto attivo sul quaderno di lavoro fino a quando non si procede con la sua gestione o assegnazione ad incaricato competente. Se il documento viene rimosso dal quaderno è sempre possibile ricercarlo in archivio documentale.

- **Presa in carico del documento se di propria competenza**
  Ciascun documento pervenuto deve essere preso in carico dall'operatore competente tramite l'apposita funzione. La presa in carico viene automaticamente comunicata sul quaderno di lavoro a tutti gli operatori abilitati alla visione/gestione di quel documento.
- **Fascicolazione digitale del documento**
  L'operazione di fascicolazione digitale avviene con le modalità descritte nel capitolo *"4. Fascicolazione di un documento"* del presente allegato.
- **Assegnazione di un documento ad incaricato del procedimento**
  Il Responsabile di un'unità organizzativa può assegnare un documento ricevuto ad uno o più incaricati del procedimento, i quali lo ricevono in apposito nodo del quaderno di lavoro. Le modalità di gestione sono descritte nel capitolo "*7. Assegnazione dei documenti"* del presente allegato.
- **Inoltro a soggetti esterni all'AOO;**
  All'interno del sistema documentale è possibile inviare all'esterno dell'AOO qualsiasi documento ricevuto. L'invio potrà avvenire per via telematica (E-mail, E-mail certificata...)
- **Risposta al documento ricevuto**
  Il documento ricevuto può essere evaso rispondendo con un nuovo documento e indicando la modalità con cui si è evasa la documentazione. Le modalità di gestione sono descritte nel capitolo *"3 "Inserimento/Formazione di un nuovo documento"* del presente allegato.

12. Operatività del flusso dei documenti da trasmettere

Il sistema documentale permette di creare un documento in risposta ad uno ricevuto.
Esistono diverse modalità per inserire un nuovo documento in OLIMPO: Le modalità di gestione sono descritte nel capitolo *"3. Inserimento/Formazione di un nuovo documento"* del presente allegato.

Dopo aver individuato la tipologia di documento che si desidera creare/utilizzare è necessario compilare e verificare i dati della maschera di dettaglio del documento, contenente i metadati con tutte le informazioni.
Nel caso di risposta a documento in entrata, questi dati sono già proposti in automatico dal sistema sulla maschera di dettaglio del nuovo documento e riportati automaticamente sul testo (qualora si scia scelto di partire da un modello predisposto);
Il testo così creato può essere redatto dall'operatore competente.
La risposta ad un documento propone automaticamente l'eventuale evasione dell'istanza ricevuta.

Le operazioni che possono essere effettuate su un documento in redazione sono le seguenti:

- **Condivisone/assegnazione di un documento all'interno dell'AOO**
  Le modalità di gestione sono descritte nei capitoli *"6. Condivisione dei documenti"* e "*7. Assegnazione dei documenti"* del presente allegato.
- **Fascicolazione digitale del documento**

L'operazione di fascicolazione digitale avviene con le modalità descritte nel capitolo *"4. Fascicolazione di un documento"* del presente allegato.

- **Firmare digitalmente i file di un documento**
  Previo inserimento di un dispositivo di firma digitale nel PC è possibile firmare digitalmente i file di un documento in OLIMPO sfruttando la funzione di firma automatica cos' come specificato nel capitolo *"8. Sottoscrizione documenti informatici"* del presente allegato.

- **Protocollare automaticamente il documento in uscita**
  All'interno del sistema documentale è possibile, da parte degli utenti preventivamente abilitati dal Responsabile del protocollo, protocollare in uscita i documenti. Utilizzando la funzione di protocollazione automatica viene visualizzata la maschera del protocollo comprensiva di tutti i dati già preventivamente caricati dall'utente sul documento e si può attribuire il numero di protocollo.
  I riferimenti del protocollo vengono poi riportati automaticamente all'interno del file sul quale si stava lavorando (*se si trattava di modello di testo predisposto*).
  Se l'utente non è abilitato alla protocollazione può comunque inoltrare il documento tramite il sistema documentale all'ufficio protocollo, il quale vedrà la richiesta in uno specifico nodo sul quaderno di lavoro e potrà protocollare il documento.

- **Archiviare un documento**
  Terminate le operazioni di redazione del documento si può procedere all'archiviazione del medesimo. A ciascun documento archiviato viene attribuito un codice univoco di archiviazione.

- **Invio del documento ai destinatari**
  È possibile inviare all'esterno dell'AOO qualsiasi documento creato all'interno del sistema documentale. Se la trasmissione avviene per via telematica (e-mail, e-mail certificata,...), il messaggio di posta elettronica viene automaticamente salvato all'interno del documento inviato, così come le ricevute di accettazione e consegna qualora l'invio avvenga tramite Posta Elettronica Certificata.

COMUNE DI GRIGNASCO

ALLEGATO 8

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

IL SISTEMA DI CONSERVAZIONE ADOTTATO DALL'ENTE

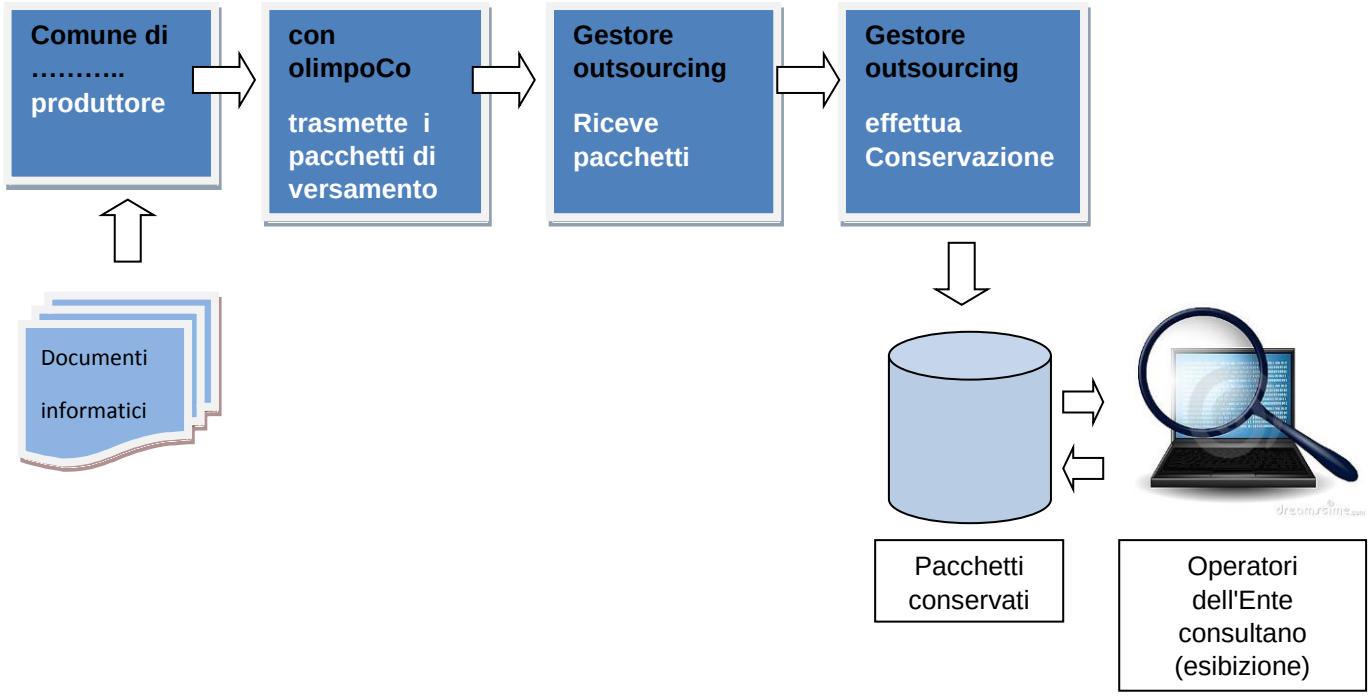
Indice

1 La conservazione dei documenti informatici dell'Ente

1.1 Il sistema di conservazione adottato dall'Ente

L'Ente affida il servizio di conservazione ad un conservatore accreditato esterno.

Il "ciclo di gestione della conservazione" in outsourcing realizzato da con conservatore accreditato



Il sistema prevede la "gestione del ciclo della conservazione"… dal reperimento dei documenti e la preparazione dei pacchetti di versamento, fino alla conservazione a **norma** effettuata **c/o outsourcer esterno accreditato** che viene nominato responsabile della conservazione.

1.2 Il sistema di versamento organizzato dall'Ente

Il sistema di versamento adottato dall'Ente è il sistema OlimpoCoOutosurcer che consente la gestione completa del flusso di versamento: creazione pacchetti, trasmissione tramite interfaccia al conservatore, archiviazione ricevute e monitoraggio operatività.
Ogni servizio produttore di documenti informatici è anche responsabile del procedimento di trasmissione dei pacchetti di versamento di propria competenza al conservatore esterno.

Modulo adottato: software OlimpoCo per produzione/trasmissione pacchetti di versamento all'outsourcer.

Le tipologie documentarie prodotte dall'Ente, da conservare, sono numerose (contratti, fatture, registri, atti, provvedimenti, etc.).

Pertanto si rende necessario avere un sistema che gestisce la conservazione di questo universo di documenti in modo programmato.

Nel contesto del ciclo di conservazione riveste particolare importanza la gestione della fase di versamento che prevede :

- Programmazione delle tipologie dei documenti da conservare
- Scadenziario per tipologia documentaria
- Preparazione dei pacchetti di versamento per il sistema di conservazione con le specifiche tecniche definite con l'outsourcer
- Registro delle avvenute conservazioni

Il modulo adottato è altamente qualificato per gestire il versamento dei documenti informatici in modo automatico, controllato con lo scadenziario ed il periodo di conservazione.

La gestione dei pacchetti di versamento avviene tramite il sistema di interscambio "OlimpoCoOutsourcer" che gestisce i pacchetti di versamento da conservare interfacciandosi con le procedure Siscom e con la piattaforma di gestionale documentale.

1.3 Il sistema di esibizione pacchetti di distribuzione

La consultazione dei documenti conservati dei pacchetti di distribuzione (esibizione) è accedibile tramite il sistema on-line messo a disposizione dall'Outsourcer con abilitazione tramite autentica degli operatori delegati dall'ente.

I soggetti abilitati alla consultazione dei pacchetti di distribuzione (esibizione) sono comunicati all'Outsourcer contestualmente alla modulistica di adesione al servizio.

2 Manuale della conservazione

Viene adottato il Manuale della conservazione dell'Outsourcer a cui viene affidato il servizio pubblicato su sito web dell' Agid.

L'Ente definisce nella gestione del manuale di gestione documentale i procedimenti di versamento e di rapporti operativi con il Conservatore esterno.

3 Responsabile della conservazione

L'ente nomina come "Responsabile della conservazione" il Responsabile della conservazione dell'Outsourcer a cui affida il servizio.

Il Responsabile della gestione documentale è anche responsabile della conservazione interna, limitatamente alle funzioni di coordinamento e supervisione del sistema realizzato dall'Ente per la gestione delle operazioni di Versamento dei pacchetti da conservare trasmessi al conservatore.
Il Responsabile della conservazione interno tiene i rapporti con il personale dei servizi per le operazioni di versamento.

4 Specificità per la conservazione del registro di protocollo informatico

In adempimento a quanto previsto dal D.P.C.M. 03 dicembre 2013 art. 7 c. 5, l'Ente provvede ad effettuare la conservazione del registro giornaliero di protocollo utilizzando il sistema di conservazione generale dell'Ente.
L'operazione di conservazione del registro di protocollo comprende:
- l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno
- la trasmissione entro la giornata lavorativa successiva, al sistema di conservazione OlimpoConserve, garantendo l'immodificabilità del contenuto.

Il responsabile di protocollo, direttamente o tramite suoi incaricati, provvede tramite specifica funzione programmata del sistema di protocollo, interfacciata con il software di OlimpoConserve, alla creazione del pacchetto di versamento del registro di protocollo del giorno precedente, per la verifica e la trasmissione al sistema di conservazione. Lo stesso soggetto e' tenuto al monitoraggio dell'esito positivo delle operazioni di avvenuta conservazione.

5 Gestore del servizio in outsourcing dell'Ente

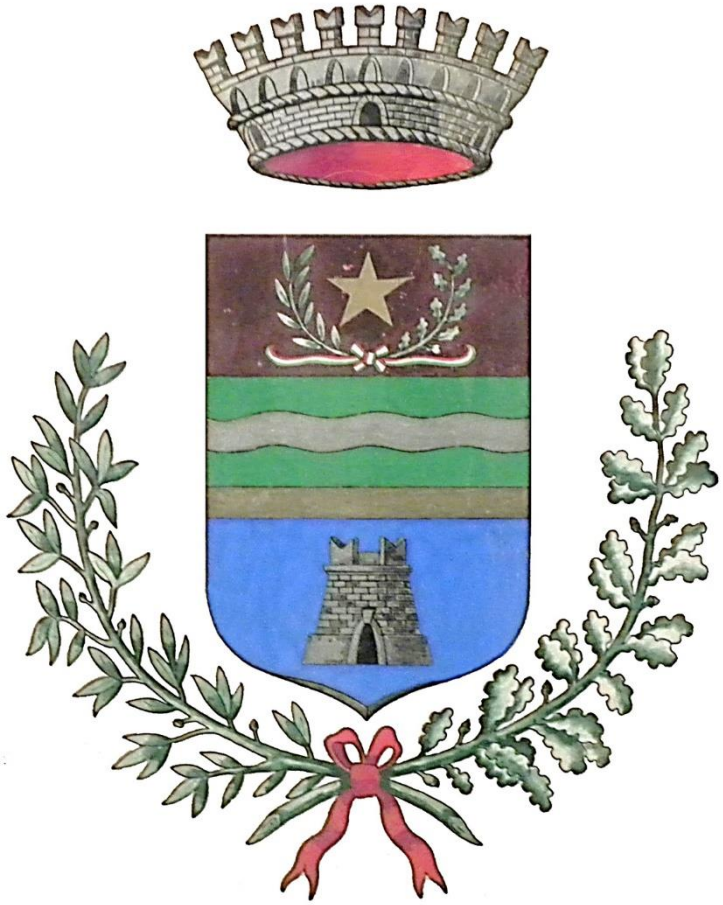
L'Ente tiene un registro nel quale vengono riportati i riferimenti ai conservatori esterni a cui e' affidata la conservazione con le date di incarico e di inizio attività ed eventuale fine incarico. Tale registro viene mantenuto aggiornato dal Responsabile della gestione documentale.

COMUNE DI GRIGNASCO

ALLEGATO 9

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

STEMMA DELL'ENTE



COMUNE DI GRIGNASCO

ALLEGATO 10

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

DOCUMENTO DI PUBBLICA SICUREZZA

COMUNE DI GRIGNASCO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ARTICOLI 34 DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E 19 DEL DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

Sommario

Premesse

L'articolo 34, lettera g) del Codice in materia di protezione dei dati personali (D. Lgs. 196/2003) dispone che "*il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: ... g) tenuta di un aggiornato documento programmatico sulla sicurezza; ...*".

In particolare, l'articolo 19 del Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B) del Codice) prevede che: "*entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato".

L'ente si è attivato per adempiere nel miglior modo a tale obbligo, effettuando un'attività di analisi dell'organizzazione, dei trattamenti e del sistema informativo, l'analisi dei rischi e redigendo il presente documento che rappresenta la formale redazione del Documento Programmatico sulla Sicurezza ai sensi delle norme citate.

Struttura organizzativa del Comune di GRIGNASCO

L'organigramma seguente indica i settori e gli uffici preposti ai trattamenti di dati per le funzioni istituzionali dell'ente. Di seguito viene, inoltre, individuato l'elenco del personale appartenente ai settori/uffici (l'elenco degli incaricati del trattamento di cui al Disciplinare Tecnico in materia di misure minime di sicurezza).

FIGURA PROFESSIONALE	**AREA DI APPARTENENZA**	**NOMINATIVO DIPENDENTE**
Segretario Comunale	Polizia urbana-Asilo Nido Comunale – Biblioteca – Servizi Scolastici - personale	Regis Milano dott. Michele
Istruttore direttivo	Area Amministrativa	Bonazzi Valentina
Istruttore	Area Demografici	Savioli Francesca
Applicato / Autista / Informagiovani	Area Amministrativa	Garino Marco
Istruttore	Area Polizia Urbana	Sartori Paolo
Istruttore	Area Polizia Urbana	Alberti Mirko
Istruttore direttivo	Area Ufficio tecnico	Faccini Milver
Istruttore	Area Ufficio tecnico	Mastropasqua Angela
Istruttore	Area Ufficio tecnico	Cacciami Anna
Operaio cantoniere / Autista	Area Ufficio tecnico	Ghiringhelli Massimo
Operaio cantoniere/ Autista	Area Ufficio tecnico	Pedriali Stefano

Operaio cantoniere	Area Ufficio tecnico	Mortarotti Lorenzo
Operaio specializzato	Area Ufficio tecnico	Bressan Daniele
Applicato cimitero	Area Ufficio tecnico	Fioro Eraldo
Educatrice d'infanzia	Area Segreteria	Mascio Nicoletta
Educatrice d'infanzia	Area Segreteria	Nobili Sabrina
Educatrice d'infanzia	Area Segreteria	Tiramani Annamaria
Cuoca	Area Segreteria	Cortis Paola
Cuoca	Area Segreteria	Morgoni AnnaPaola
Biblioteca	Area Segreteria	Gobbi Laura
Ragioneria	Area Contabile	Chiappini Laura
Tributi	Area Contabile	Morgoni Barbara

1. Elenco dei trattamenti di dati personali

Nel presente capitolo, conformemente all'articolo 19.1. del Disciplinare Tecnico in materia di misure minime di sicurezza, è riportato l'elenco dei trattamenti di dati personali cui sono preposti gli uffici e relativo personale incaricato.

Per la definizione dei trattamenti sono state utilizzate alcune definizioni previste ai fini della notificazione al Garante per la protezione dei dati personali in vigenza della L. 675/1996 nonché le definizioni tratte dall'indice dei trattamenti della bozza di "*REGOLAMENTO RELATIVO ALL'IDENTIFICAZIONE DELLE ATTIVITÀ CHE PERSEGUONO RILEVANTI Finalità DI INTERESSE PUBBLICO, AI SENSI DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196*" pubblicato dall'ANCI (Associazione Nazionale Comuni Italiani) sul sito Internet http://www.ancitel.it/regolamentodatisensibili/indice_trattamenti.asp.

Conformemente alle indicazioni fornite dal Garante per la protezione dei dati personali (13 maggio 2004), l'elenco riporta i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della struttura (o reparto, funzione, ufficio, ecc.) interna od esterna che operativamente effettua il trattamento e della natura dei dati trattati. In particolare, l'elenco riporta le seguenti informazioni, ritenute "essenziali" dall'Autorità:
Identificativo del trattamento: consistente in un codice utile per un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle (il codice corrisponde al numero del paragrafo di riferimento);
Descrizione sintetica: descrizione del trattamento in modo da consentire una comprensione immediata della tabella;
Struttura di riferimento: indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento. In caso di compartecipazione di più strutture saranno indicate tutte le strutture di riferimento.
Natura dei dati trattati: indicazione della tipologia di dati oggetto del singolo trattamento elencato (dati comuni, sensibili o giudiziari);
Banca dati: il nome o l'identificativo dell'eventuale banca dati (ovvero del data base o dell'archivio informatico) in cui sono contenuti i dati che sono trattati. Qualora un trattamento richieda l'utilizzo di dati che risiedono in più banche dati saranno elencate le diverse banche dati;
Ubicazione fisica dei supporti di memorizzazione: contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cioè dove si trova (in quale sede, centrale o periferica, presso quale fornitore di servizi, etc.) l'elaboratore sui cui dischi sono memorizzati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, Cd, ecc.);
Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento;
Tipologia di interconnessione: descrizione sintetica e qualitativa della rete informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati: rete locale, Extranet, Internet, ecc..

L'aggiornamento delle informazioni contenute nelle successive tabelle coincide con la data di formalizzazione del presente documento.

1.1. Trattamento giuridico ed economico del personale

DESCRIZIONE DEL TRATTAMENTO
Per trattamento giuridico ed economico del personale si intende, a titolo esemplificativo e non esaustivo, il calcolo e il pagamento di retribuzioni, l'applicazione della legislazione previdenziale ed assistenziale nonché il riconoscimento di benefici connessi all'invalidità civile per il personale.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Segreteria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*
Informa Srl	X	

CATEGORIE DI INTERESSATI
Personale dipendente
Familiari dell'interessato

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati dipendenti comune	Disco z	Sede Comune
Banca dati rilevazione presenze	Disco z	Sede Comune
Banca dati back up	Supporto magnetico	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio trattamenti giuridici ed economici dei dipendenti	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.2. Concorsi pubblici per l'assunzione del personale

DESCRIZIONE DEL TRATTAMENTO
Per concorsi pubblici per l'assunzione del personale si intendono i processi di gestione e amministrativa dei concorsi pubblici pubblicati per la ricerca di nuovo personale.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Segreteria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Candidati

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
File verbali concorsi	Disco z	Sede Comune
Banca dati back up	server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio concorsi pubblici	Archivio Generale ufficio tecnico	Sede Comune
Archivio del Personale	Archivio Generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.3. Concorsi interni e formazione del personale

DESCRIZIONE DEL TRATTAMENTO
Per concorsi interni si intendono i processi di promozione del personale a seguito del superamento di specifici concorsi di selezione. Per formazione del personale si intendono i processi di programmazione di corsi di formazione in aula o presso strutture esterne al comune per il personale dipendente.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area segreteria	x	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Dipendenti

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti

Dati sensibili	Non presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
File verbali concorsi	Disco z	Sede Comune
Banca dati back up	server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio concorsi ed assunzioni	Archivio Generale ufficio tecnico	Sede Comune
Corsi di formazione	Archivio Generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.4. Adempimenti contabili e fiscali

DESCRIZIONE DEL TRATTAMENTO
Per adempimenti contabili e fiscali si intendo tutti i processi inerenti alla contabilità e amministrazione dell'Ente

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Ragioneria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*
Tesoreria comunale – Banco Popolare	x	

CATEGORIE DI INTERESSATI
Fornitori
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati debitori (applicativo Siscom/Giove)	Server	Sede Comune
Banca dati creditori (applicativo Siscom/Giove)	Server	Sede Comune
Banca dati fornitori (applicativo Siscom/Giove)	Server	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati debitori	Archivio Generale ufficio tecnico	Sede Comune
Banca dati creditori	Archivio Generale ufficio tecnico	Sede Comune
Banca dati fornitori	Archivio Generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.5. Ordine e sicurezza pubblica

DESCRIZIONE DEL TRATTAMENTO
Per attività di ordine e sicurezza pubblica si intendono i processi di gestione delle misure di sicurezza, delle misure di prevenzione, accertamento e repressione dei reati.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Polizia Urbana	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati back up	server	
Banca dati fornitori (applicativo "Concilia " Maggioli)	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati verbali di contestazione alle violazioni del Codice stradale	Archivio Ufficio Servizio Vigilanza	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.6. Amministrazione della popolazione

DESCRIZIONE DEL TRATTAMENTO
Per amministrazione della popolazione si intendono i processi di gestione delle anagrafi della popolazione e dei registri dello stato civile; rilascio di certificati ed estratti.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Demografici	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati demografico (applicativo Siscom)	Server	Sede Comune
Banca dati demografica (applicativo Siscom)	Server	Sede Comune
Database Anagaire (applicativo Siscom)	Server	Sede Comune
Stato civile (Applicativo Siscom)	Server	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati della popolazione residente / pratiche immigrazione - emigrazione	Archivio generale ufficio tecnico	Sede Comune
Cartellini carte d'identità – Registro passaporti	Archivio generale ufficio tecnico	Sede Comune
Banca dati italiani residenti all'estero	Archivio generale ufficio tecnico	Sede Comune
Banca dati cittadini stranieri (appartenenti alla Comunità Europea ed Extracomunitari)	Archivio generale ufficio tecnico	Sede Comune
Registri degli atti di nascita – matrimonio – morte - pubblicazioni di matrimonio - cittadinanza	Archivio generale ufficio tecnico	Sede Comune
Liste di leva	Archivio generale ufficio tecnico	Sede Comune
Banca dati titolati pensioni INPS e invalidi civili	Archivio generale ufficio tecnico	Sede Comune
Archivio provvedimenti penali	Archivio generale ufficio tecnico	Sede Comune
Archivio provvedimenti sanitari	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.7. Accertamento e riscossione di tasse e imposte

DESCRIZIONE DEL TRATTAMENTO
Per accertamento e riscossione di tasse e imposte si intendono i processi di verifica della sussistenza dei requisiti per il pagamento di tasse e imposte nonché l'attività di riscossione delle stesse.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Ragioneria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*
Progel srl di Gallarate (VA)	X	

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati tributi (Applicativo Siscom)	Server	Sede Comune
Banca dati back up	Server	Sede comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati Tributi	Generale Archivio generale ufficio tecnico	sede

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.8. Autorizzazioni, concessioni, permessi, licenze e nulla-osta

DESCRIZIONE DEL TRATTAMENTO
Per autorizzazioni, concessioni, permessi, licenze e nulla-osta si intende l'adozione dei provvedimenti di rilascio e attività connesse; l'individuazione degli aventi diritto, la verifica e il controllo delle condizioni.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Polizia Urbana	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati pubblici esercizi e commercio	Disco z	Sede Comune
Banvìca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati pubblici esercizi e commercio	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.9. Attività di carattere elettorale

DESCRIZIONE DEL TRATTAMENTO
Per attività di carattere elettorale si intende la tenuta di liste elettorali, lo svolgimento di compiti pubblici relativi a consultazioni elettorali e referendarie.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Demografici	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati elettorale (Applicativo Siscom)	Server	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI

DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati degli elettori	Archivio generale ufficio tecnico	Sede Comune
Albi sezionali e generali degli elettori	Archivio generale ufficio tecnico	Sede Comune
Banca dati degli incarichi elettorali (presidenti – segretari - scrutatori di seggio)	Archivio generale ufficio tecnico	Sede Comune
Banca dati elettorale mandamentale	Archivio generale ufficio tecnico	Sede Comune
Archivio comunicazioni giudiziarie elettorali	Archivio generale ufficio tecnico	Sede Comune
Archivio comunicazioni sanitarie elettorali	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.10. Pianificazione urbanistica, amministrazione del territorio, controllo su illeciti edilizi

DESCRIZIONE DEL TRATTAMENTO
Per attività di pianificazione urbanistica, amministrazione del territorio, controllo su illeciti edilizi si intendono le attività di definizione del piano regolatore edilizio, la gestione amministrativa di immobili, terreni e proprietà dislocate sul territorio nonché il monitoraggio in merito ad eventuali illeciti edilizi o costruzioni abusive.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Ufficio Tecnico LLPP urbano edilizia	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati concessioni edilizie	Disco z	Sede Comune
Banca dati condoni edilizi	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati concessioni edilizie	Archivio generale ufficio tecnico	Sede Comune
Banca dati condoni edilizi	Archivio generale ufficio tecnico	Sede Comune
Banca dati verbali accertamenti edilizi	Archivio generale ufficio tecnico	Sede Comune

Archivi provvedimenti sanzionatori	Archivio generale ufficio tecnico	Sede Comune
Banca dati urbanistica	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connessione rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.11. Progettazione, affidamento o esecuzione di opere pubbliche

DESCRIZIONE DEL TRATTAMENTO
Per progettazione, affidamento o esecuzione di opere pubbliche si intendono le attività di pianificazione e assegnazione di appalti pubblici per la costruzione di opere pubbliche nonché per la manutenzione del patrimonio comunale.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Ufficio tecnico LLPP urbano edilizia	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati ditte per gare d'appalto	Disco Z	Sede Comune
Banca dati stato d'avanzamento lavori	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati ditte per gare d'appalto	Archivio generale ufficio tecnico	Sede Comune
Banca dati stato d'avanzamento lavori	Archivio generale ufficio tecnico	Sede Comune
Banca dati progetti	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.12. Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne

DESCRIZIONE DEL TRATTAMENTO
Per attività relativa alla gestione degli asili nido comunali, dei servizi per l'infanzia e delle scuole materne si intendono le attività inerenti la gestione amministrativa delle strutture comunali (asili, scuole materne) e dei servizi destinati alla formazione e all'istruzione dell'infanzia.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Segreteria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banca dati	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.13. Gestione delle biblioteche e dei centri di documentazione

DESCRIZIONE DEL TRATTAMENTO
Per attività di gestione delle biblioteche e dei centri di documentazione si intendono le attività di gestione amministrativa (gestione dei locali, gestione di iscritti e frequentatori) dei locali adibiti a biblioteche e centri culturali.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Segreteria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati utenti della biblioteca (Applicativo Progetto Leonardo Biblios 90)	Disco z	Sede Biblioteca
Banca dati back up	Server	Sede Biblioteca

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio utenti della biblioteca	Archivio generale Biblioteca	Sede Biblioteca

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.14. Attività artistiche, culturali, ricreative, sportive e di valorizzazione del tempo libero

DESCRIZIONE DEL TRATTAMENTO
Per attività artistiche, culturali, ricreative, sportive e di valorizzazione del tempo libero si intendono i processi di programmazione e organizzazione di eventi culturali e ricreativi (quali ad esempio, il teatro, il cinema e incontri formativi) nonché sportivi (quali ad esempio, tornei e campionati sportivi) sia per bambini e giovani sia per adulti e anziani.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Amministrativa	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cariche istituzionali

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*

Dati personali comuni	Presenti
Dati sensibili	Non presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati nominativi per inviti	Disco z	Sede Comune
Banca dati iniziative culturali	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio iniziative culturali	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.15. Servizi sociali e di assistenza

DESCRIZIONE DEL TRATTAMENTO
Per servizi sociali e di assistenza si intende la gestione delle attività di sostegno economico-sociale a cittadini non-autosufficienti, malati, anziani o handicappati.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Amministrativa	x	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Persone fisiche domiciliate

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati servizi sociali	Server	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio servizi sociali	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.16. Protezione civile

DESCRIZIONE DEL TRATTAMENTO
Per protezione civile si intendono gli interventi per disastri e calamità, assistenza, gestione dei sussidi e degli interventi di recupero nonché la gestione dei rapporti con il volontariato.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Ufficio tecnico LLPP	x	
Polizia urbana	x	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Cittadini
Volontari
Fornitori

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banche dati protezione civile	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Banche dati protezione civile	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.17. Gestione del contenzioso

DESCRIZIONE DEL TRATTAMENTO
Per gestione del contenzioso si intende, a titolo esplicativo ma non esaustivo, la gestione di contenziosi amministrativi, inadempimenti contrattuali di fornitori o concessionari di pubblico servizio, di diffide, di transazioni, controversie

giudiziarie in genere.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Segretario Comunale , Ufficio tecnico, Ufficio Tributi, Ufficio Segreteria dell'Area Amministrativa	x	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Dipendenti
Fornitori
Cittadini

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati dipendenti	Disco z	Sede Comune
Banca dati sinistri attivi e passivi	Disco z	Sede Comune
Banca dati affari legali	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio dipendenti comune	Archivio generale ufficio tecnico	Sede Comune
Archivio affari legali	Archivio generale ufficio tecnico	Sede Comune
Archivio sinistri	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.18. Gestione dei fornitori

DESCRIZIONE DEL TRATTAMENTO
Per gestione dei fornitori si intende a titolo esemplificativo ma non esaustivo l'amministrazione dei fornitori l'amministrazione dei contratti , la gestione degli ordini, di arrivi e di fatture.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Tutti gli uffici competenti	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Fornitori

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Non presenti
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati fornitori	Disco z	Sede Comune
Banca dati back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio fornitori	Archivio generale ufficio tecnico	Sede Comune
Archivio contratti forniture	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

1.19. Gestione del patrimonio mobiliare ed immobiliare

DESCRIZIONE DEL TRATTAMENTO
Per attività di gestione mobiliare e immobiliare si intende la gestione dei beni fisici (edifici, unità immobiliari) del patrimonio disponibile dell'Ente.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Area Ragioneria	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*

CATEGORIE DI INTERESSATI
Locatari

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Presenti
Dati giudiziari	Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE

DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Banca dati alloggi comunali	Disco z	Sede Comune
Inventario beni proprietà comunali (Applicativo Siscom)	Server	Sede Comune
Banca dati manutenzione beni immobili	Disco z	Sede Comune
Banca dati Back up	Server	Sede Comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*
Archivio contratti	Archivio generale ufficio tecnico	Sede Comune
Archivio manutenzioni	Archivio generale ufficio tecnico	Sede Comune

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*
Computer	Connesso rete lan

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO

1.20. Gestione e manutenzione del sistema informativo comunale

DESCRIZIONE DEL TRATTAMENTO
Per gestione e manutenzione del sistema informativo comunale si intendono tutte quelle operazioni atte a gestire le risorse hardware e software.

UNITÀ O AREE ORGANIZZATIVE PREPOSTE AL TRATTAMENTO		
DENOMINAZIONE UNITÀ O AREA	*OWNER*	*CONCORRENTE*
Tutte	X	

TERZI SOGGETTI PREPOSTI AL TRATTAMENTO		
DENOMINAZIONE	*TITOLARE*	*RESPONSABILE*
Consulenti esterni – Hobby PC - Siscom	x	

CATEGORIE DI INTERESSATI
Clienti
Fornitori
Dipendenti
Agenti
Utenti

NATURA DEI DATI OGGETTO DI TRATTAMENTO	
TIPOLOGIA	*PRESENZA*
Dati personali comuni	Presenti
Dati sensibili	Potenziali
Dati giudiziari	Non Presenti

BANCHE DATI E SUPPORTI DI MEMORIZZAZIONE		
DENOMINAZIONE	*ASSET DI ARCHIVIAZIONE*	*LUOGO*
Applicativo Siscom	Server	Sede del comune
Applicativo Maggioli	Server	Sede del comune
Applicativo Progetto Leonardo Biblios 90)	Server	Sede del Biblioteca
Banca dati back up	Server	Sede del comune
Banche dati office	Disco z	Sede del comune

ARCHIVI CARTACEI		
DENOMINAZIONE	*LOCALI DI ARCHIVIAZIONE*	*LUOGO*

TIPOLOGIA DI ACCESSO E INTERCONNESSIONE	
TIPOLOGIA DISPOSITIVI DI ACCESSO	*TIPOLOGIA DI INTERCONNESSIONE*

EVENTUALE SITO WEB A SUPPORTO DEL TRATTAMENTO
-

2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Ai sensi dell'articolo 19.2. del Disciplinare Tecnico in materia di misure minime di sicurezza, nei prossimi paragrafi vengono specificate le informazioni inerenti la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

2.1. Definizioni dei "Ruoli di Legge e Regolamentari"

Nel presente paragrafo si riporta l'elenco dei ruoli, e relative funzioni e competenze, previste dalla vigente normativa in materia di protezione dei dati personali:

Addetti alla custodia e gestione delle parole chiave: persone incaricate per iscritto alla custodia delle parole chiave (l'elenco degli addetti alla custodia e gestione delle parole chiave è riportato nelle apposite tabelle dei paragrafi successivi);

Amministratori di sistema: soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo e/o di gestione dei database e di consentirne l'utilizzazione (l'elenco degli amministratori di sistema è riportato nelle apposite tabelle dei paragrafi successivi);

Incaricati della manutenzione: persone addette alla manutenzione dell'hardware, del software applicativo e del software di base degli elaboratori sui quali sono memorizzati i dati personali sensibili (l'elenco degli incaricati della manutenzione è riportato nelle apposite tabelle dei paragrafi successivi);

Incaricato del trattamento: persona fisica identificata dal Titolare tramite apposita nomina che esegue le operazioni di trattamento (tutti i dipendenti e i collaboratori del titolare che, per mansioni, effettuano operazioni di trattamento di dati personali; l'individuazione per iscritto di tali soggetti è riscontrabile nelle lettere di incarico formalizzate per iscritto; l'elenco degli incaricati è riportato nelle apposite tabelle dei paragrafi successivi);

Responsabile del trattamento: persona fisica o giuridica o altro organismo preposto dal titolare al trattamento dei dati personali. I compiti affidati al responsabile devono essere specificati analiticamente per iscritto (l'elenco dei responsabili del trattamento è riportato nelle apposite tabelle dei paragrafi successivi);

Responsabile della struttura: persona fisica dirigente o responsabile della struttura organizzativa di riferimento, a prescindere dall'eventuale nomina di responsabile del trattamento (l'elenco dei responsabili di struttura è riportato nelle apposite tabelle dei paragrafi successivi);

Titolare: persona fisica o giuridica o altro organismo cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, compreso il profilo della sicurezza.

2.2. Tabelle di distribuzione dei compiti e delle responsabilità.

Nei successivi paragrafi, conformemente alle indicazioni fornite dal Garante per la protezione dei dati personali (13 maggio 2004), si riportano le tabelle che associano ad ogni struttura (o settore, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità ai sensi della normativa.

La data di aggiornamento delle informazioni contenute nelle tabelle è quella indicata quale data di emissione del documento.

2.2.1 Segretario Comunale

PERSONALE PREPOSTO	
COGNOME E NOME	**FUNZIONE**
Regis Milano dott. Michele	Segretario Comunale

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
In ragione del proprio ruolo, il segretario comunale ha accesso a tutti i dati trattati dall'Ente Responsabile Polizia urbana , Asilo Nido Comunale, Biblioteca e Scuole Personale

2.2.2 Area Amministrativa

PERSONALE PREPOSTO	
COGNOME E NOME	**FUNZIONE**
Bonazzi Valentina	Incaricato del Trattamento
Garino Marco	Incaricato del Trattamento

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Trattamento giuridico del personale
Concorsi pubblici per assunzione del personale
Concorsi interni e formazione del personale
Attività artistiche, culturali, ricreative, sportive, e di valorizzazione del tempo libero
Servizi Sociali e di assistenza
Attività amministrativa

2.2.3 Area Demografici

PERSONALE PREPOSTO	
COGNOME E NOME	**FUNZIONE**
Bonazzi Valentina	Incaricato del Trattamento
Savioli Francesca	Incaricato del Trattamento
Sartori Polo	Incaricato del Trattamento

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Amministrazione della Popolazione
Attività di carattere Elettorale

2.2.4 Area Polizia urbana

PERSONALE PREPOSTO

COGNOME E NOME	FUNZIONE
Sartori Paolo	Incaricato del Trattamento
Alberti Mirko	Incaricato del Trattamento

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Ordine e sicurezza pubblica
Autorizzazioni , concessioni, permessi, licenze e nulla-osta
Protezione civile

2.2.5 Area Ufficio Tecnico L.L.P.P. Urbana edilizia

PERSONALE PREPOSTO	
COGNOME E NOME	FUNZIONE
Faccini Milver	Incaricato del Trattamento
Ghiringhelli Massimo (dato in convenzione al Comune di Maggiora)	Incaricato del Trattamento
Pedriali Stefano	Incaricato del Trattamento
Bressan Daniele	Incaricato del Trattamento
Fiorio Eraldo	Incaricato del Trattamento
Mortarotti Lorenzo	Incaricato del Trattamento
Mastropasqua Angela	Incaricato del Trattamento
Cacciami Anna	Incaricato del Trattamento
Fasola Elisabetta (Convenzione Comune di Boca)	Incaricato del Trattamento

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Pianificazione urbanistica, amministrazione del Territorio e controllo sugli illeciti edilizi
Progettazione, affidamento o esecuzione di opere pubbliche
Protezione Civile
Gestione dei fornitori
Gestione del contenzioso

2.2.6 Area Ragioneria

PERSONALE PREPOSTO	
COGNOME E NOME	FUNZIONE
Franzini Annalisa (Convenzione con Comune di Maggiora)	Incaricato del Trattamento
Morgoni Barbara	Incaricato del Trattamento
Chiappini Laura	Incaricato del Trattamento

TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Adempimenti contabili e fiscali
Accertamento e riscossione tasse e imposte

2.2.7 Area Segreteria

PERSONALE PREPOSTO	
COGNOME E NOME	FUNZIONE
Regis Milano dott. Michele	Incaricato del Trattamento
Gobbi Lara Anna	Incaricato del Trattamento
Mascio Nicoletta	Incaricato del Trattamento
Nobili Sabrina	Incaricato del Trattamento
Tiramani Anna Maria	Incaricato del Trattamento
Cortis Paola	Incaricato del Trattamento

PERSONALE PREPOSTO	
COGNOME E NOME	FUNZIONE
Morgoni Anna Paola	Incaricato del Trattamento

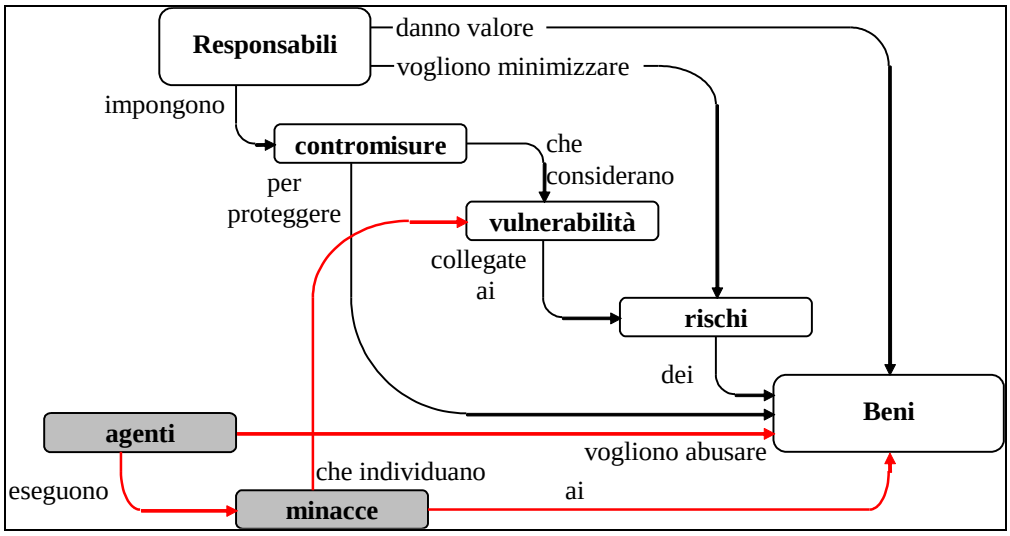
TRATTAMENTI CUI È PREPOSTA LA STRUTTURA
Attività relativa alla gestione degli asilo nido e dei servizi per l'infanzia
Gestione della Biblioteca e dei centri di documentazione servizi scolastici

Analisi dei rischi che incombono sui dati

Conformemente al disposto di cui all'articolo 19.3. del Disciplinare Tecnico in materia di misure minime di sicurezza il presente capitolo riporta gli esiti dell'attività di analisi dei rischi che incombono sui dati. Prima dell'esposizione dei risultati di tale attività, nel successivo paragrafo si riportano alcuni riferimenti in merito alla metodologia utilizzata per effettuare l'analisi.

3.1. Metodologia

L'attività di analisi dei rischi è stata svolta ai fini dell'adempimento agli obblighi di cui alla normativa in materia di protezione dei dati personali. In quest'ottica, l'analisi si è basata su uno schema logico che può essere riassunto dal grafico successivo:



In considerazione dello schema sopra esposto, si ricava che l'analisi dei rischi consiste nella valutazione sistematica dei seguenti fenomeni:

- la reale probabilità che tale evento minaccioso accada;
- il possibile danno derivante dalla realizzazione di un evento minaccioso;
- il livello di protezione degli asset del sistema informativo aziendale che possono prevenire l'impatto, ovvero mitigarne le conseguenze.

In considerazione di quanto sopra, la valutazione del rischio è stata valutata sulla base della seguente formula:

R = F(Minaccia, Vulnerabilità, Impatto)

L'utilizzo di un siffatto sistema di analisi e calcolo, permetterà di confrontare nel tempo gli esiti dell'analisi, di facilitarne l'aggiornamento e permetterne la verifica anche da parte di terzi.

In tale ottica, prima di passare all'esposizione della metodologia seguita, è opportuno riportare la definizione di alcuni termini fondamentali:

Minaccia: può consistere in un'azione o un potenziale evento nocivo in danno di un asset, caratterizzato da una frequenza di avvenimento (possono consistere in eventi naturali, tecnologici, umani, a loro volta distinti in volontari o involontari);

Vulnerabilità: consistente nella deficienza di security che rende possibile l'accadimento di una minaccia e ne amplia gli effetti;

Impatto: consiste nel danno (o altro effetto negativo) derivante dall'accadimento di un incidente di sicurezza;

Rischio di sicurezza: è la possibilità che una determinata minaccia si avvantaggi delle vulnerabilità per provocare un incidente, con conseguenze dannose o negative (impatto).

3.1.1. Elenco delle Minacce e tipi di impatto

L'attività di analisi dei rischi è stata svolta considerando il seguente elenco di minacce che incombono sui dati e sugli asset del sistema informativo dell'Ente. La tabella specifica anche il tipo di impatto che l'avverarsi dell'evento minaccioso può comportare sui dati personali.

Per intelligibilità della tabella si precisa che:
per "**Disponibilità**" si intende l'assicurare che gli utenti autorizzati abbiano l'accesso alle informazioni e agli asset associati quando necessario (ai sensi dell'articolo 31 del Codice, correlata al rischio di "*perdita o distruzione, anche accidentale, dei dati*");
per "**Riservatezza**" si intende il garantire che le informazioni siano accessibili solo dalle persone autorizzate ad averne l'accesso (ai sensi dell'articolo 31 del Codice, correlata al rischio di "*accesso non autorizzato*");
per "**Integrità**" si intende il proteggere l'esattezza e la completezza delle informazioni e le modalità di trattamento delle stesse (ai sensi dell'articolo 31 del Codice, correlata al rischio di "*trattamento non consentito o non conforme alle finalità della raccolta*").

	Evento	**Livello di Impatto sulla sicurezza (in termini di business, conseguenze legali e immagine)**		
		Riservatezza	**Integrità**	**Disponibilità**
Minacce informatiche	Scambio di credenziali di autenticazione tra colleghi	5	4	3
	Accessi esterni non autorizzati	5	4	3
	Ricezione e azione di virus informatici	5	5	5
	Intercettazione di informazioni riservate	5	N/A	N/A
	Incidenti, guasti malfunzionamenti tecnici	3	4	4
	Mancanza o fallimento di connessioni	N/A	2	5
Minacce naturali	Incendio	N/A	5	5
	Allagamento	N/A	5	5
	Disastri naturali	N/A	5	5
	Mancanza di energia elettrica	N/A	3	3
	Mancanza di aria condizionata in locali critici	N/A	3	3
Minacce Umane	Furto di dati da parte di personale interno	N/A	N/A	4
	Furto di dati da parte di personale esterno	N/A	N/A	4
	Danneggiamento volontario di personale interno a beni aziendali	N/A	4	5
	Danneggiamento volontario di terzi soggetti a beni aziendali	N/A	4	5
	Errori di manutenzione ai sistemi informativi	4	4	4
	Errori di utenti nelle operazioni di elaborazione dei dati	4	4	4
	Cattivo utilizzo di risorse di sistema	4	4	4
	Uso non autorizzato di applicazioni	5	5	4

3.1.2. Metodo di analisi

Come indicato nella formula precedente, la misurazione e la classificazione dei rischi incombenti sul sistema informativo dell'Ente e sulle informazioni con esso trattate si sono ottenute rapportando la probabilità che una minaccia si verifichi con il livello di vulnerabilità dell'asset stesso e il probabile impatto previsto in caso di incidente di security.

Per raggiungere tali risultati si è quindi proceduto attraverso l'esecuzione di determinate fasi operative:

1. Identificazione dei beni da proteggere (o asset del sistema informativo):
    a. *Personale;*
    b. *Processi (trattamenti);*
    c. *Risorse Fisiche;*
    d. *Risorse Hardware;*
    e. *Risorse Software;*
2. Identificazione delle minacce, assegnando a ciascuna un valore probabilistico (su scala da 1 a 5, "Irrilevante"/"Basso"/"Medio"/"Alto"/"Critico") circa il verificarsi, in base ai seguenti parametri:
    a. *Storia o statistica aziendale o di contesto;*
    b. *Contesto economico e/o geografico;*
3. Individuazione del livello di vulnerabilità (su scala da 1 a 5, "Irrilevante"/"Basso"/"Medio"/"Alto"/"Critico"):
    a. *mediante l'analisi delle contromisure implementate*;
4. Individuazione del livello di impatto (su scala da 1 a 5, "Irrilevante"/"Basso"/"Medio"/"Alto"/"Critico") che la realizzazione di un incidente di sicurezza potrebbe causare, considerando i possibili effetti legali, effetti sul business e sull'immagine della società in relazione agli obiettivi di sicurezza, ovvero:
    a. *Riservatezza;*
    b. *Integrità;*
    c. *Disponibilità;*
5. Misurazione e classificazione dei rischi mediante l'applicazione della formula sopra indicata.

L'analisi dei rischi è stata quindi calcolata attraverso una matrice, la cui base di calcolo consiste nella formula esposta in precedenza:

R=(Probabilità Minaccia x Livello di Vulnerabilità x Livello di Impatto)

Attraverso tale metodologia è stato possibile effettuare una valutazione e una classifica dei rischi del sistema informativo dell'Ente in tutte le sue principali componenti, utilizzando dati omogenei e confrontabili, utili al fine di proporre e stabilire una efficace politica aziendale di sicurezza.

La matrice, infatti, permette di evidenziare il livello di ciascun rischio e classificarlo, evidenziando altresì una classifica utile per stabilire le priorità di intervento. Le ulteriori informazioni, indicate in matrice quali elementi del calcolo del Livello di Rischio, permettono di assumere decisioni in merito alla politica da assumere in relazione al rischio inerente ciascuna minaccia. In tale ottica, per esempio, in caso di probabilità bassa di un evento minaccia con impatti elevati (incendi, allagamenti, ecc.) è stato possibile decidere per un politica di trasferimento del rischio attraverso polizze assicurative, per minacce con elevato livello di probabilità, impatto medio ed elevato livello di vulnerabilità si è deciso in favore di una politica di implementazione di ulteriori contromisure, mentre in caso di livelli bassi di impatto e probabilità e bassi o medi di vulnerabilità si è scelto di assumersi il rischio.

Per motivi di intelligibilità, di economia testuale e conformità normativa (in particolare alle disposizioni di cui all'articolo 31 del Codice in materia di protezione dei dati personali), le matrici sono state riorganizzate affinché i dati (originariamente espressi in termini numerici) siano immediatamente interpretabili e siano parametrabili rispetto ai criteri disposti dall'articolo 31 del Codice: **Disponibilità** (distruzione o perdita anche accidentale di informazioni), **Riservatezza** (accesso non autorizzato) e **Integrità** (trattamento non consentito o non conforme alle finalità della raccolta).

L'attribuzione del valore intelligibile è stata effettuata sulla base dei seguenti rapporti tra valore indicato e possibile valore numerico del Livello di Rischio:

VALORE INDICATO	VALORE DI RIFERIMENTO
Irrilevante	1 – 2,999
Basso	3 – 11,999
Medio	12 – 39,999
Alto	40 – 74,999
Critico	75 - 125
N/A	La Minaccia non impatta sul

	parametro

Nella matrice finale si è deciso di riportare anche il valore del Livello di Vulnerabilità rispetto a ciascuna minaccia, in quanto tale livello è rappresentativo dell'impegno di un'organizzazione rispetto alla problematica della sicurezza. Il livello di vulnerabilità degli asset rispetto alle possibili minacce è infatti valutabile in relazione alle contromisure (di natura organizzativa, fisica e tecnologica) adottate dall'organizzazione stessa. L'abbattimento del livello di vulnerabilità è la prima componente su cui può agire direttamente l'organizzazione per ridurre i rischi legati al trattamento delle informazioni dipendenti dal sistema informativo aziendale (e relativi asset).

L'attribuzione del valore intelligibile è stata effettuata sulla base dei seguenti rapporti tra valore indicato e possibile valore numerico del Livello di Vulnerabilità:

VALORE INDICATO	VALORE DI RIFERIMENTO
Irrilevante	1
Basso	>1 – <3
Medio	>3 – <4
Alto	>4 – <5
Critico	5

3.2. Perimetro di applicazione dell'attività di analisi del rischio

3.2.1. Identificazione e classificazione degli asset sottoposti all'attività di analisi del rischio

Il primo passo da compiere nell'attività di analisi del rischio è l'individuazione e la classificazione degli elementi del sistema informativo che necessitano di protezione.

Nei paragrafi successivi vengono identificati e classificati per macro categoria gli asset del sistema informativo dell'Ente oggetto dell'attività di analisi del rischio.

Nel capitolo 4, viene analizzato il livello di vulnerabilità di ciascun asset in funzione delle differenti tipologie di minacce informatiche, naturali o umane cui possono essere sottoposti tali asset.

3.2.1.1. EDIFICI

EDIFICI			
Descrizione	**Indirizzo**	**N.**	**Città**
Municipio	Via V. Emanuele II	15	Grignasco
Sede polizia municipale	Via V. Emanuele II	15	Grignasco
Biblioteca Comunale	Piazza Cacciami	10	Grignasco
Asilo Nido Comunale	Via C. Battisti	22	Grignasco

3.2.1.2. UFFICI E LOCALI DI PARTICOLARE CRITICITÀ

LOCALI CON PARTICOLARI REQUISITI DI SICUREZZA				
Descrizione	**Sede**	**Dati Sensibili o Riservati**	**Sistema Controllo Accessi**	
			Si/No	**Tipo**
Ufficio Personale	Sede	Sensibili	no	-
Ufficio Anagrafe	Sede	Sensibili	no	
Ufficio Tributi	Sede	Sensibili	No	
Ufficio Assistenza	Sede	Sensibili	No	

3.2.1.3. LOCALI SERVER

LOCALI SERVER			
Descrizione	**Edificio**	**Sistema Controllo Accessi**	
		Si/No	**Tipo**
Locale dedicato con accesso dall'Ufficio Anagrafe	Sede	no	

3.2.1.4. SERVER

SERVER			
Denominazione	**Localizzazione**	**Funzione**	**Database**
Server	Locale dedicato con accesso dall'Ufficio Anagrafe	Banca dati applicativi	Applicativi gestionali

SERVER		
Denominazione	**Sistema Operativo**	**Antivirus**
Server	Windows NT	SI

3.2.1.5. CLIENT

ELABORATORI CLIENT				
Sistema Operativo	Aggiornamenti Annuali		Antivirus	
	Periodicità	Tipo	Si/No	Versione
Windows Xp	Automatico	Automatico	Si	Norton
Windows 7	Automatico	Automatico	Si	Norton

3.2.1.6. APPLICATIVI SPECIALI

APPLICATIVI SPECIALI					
Descrizione	Attribuzione	Autenticazione		Profilazione autonoma	
		Si/No	Tipo	Si/No	Tipo
Gestionali	Tutte le aree	si	Profilo utenti	si	psw

3.2.1.7. DATABASE

DATABASE			
Descrizione	Funzione	Collocazione	Area o Servizio di attribuzione

3.2.1.8. ARCHIVI CARTACEI DI PARTICOLARE IMPORTANZA O CRITICITÀ

ARCHIVI CARTACEI					
Descrizione	Attribuzione	Dati Sensibili o Riservati		Controllo Accessi	
		Si/No	Tipo	Si/No	Tipo
Archivio comunicazioni giudiziarie elettorali Archivio comunicazioni sanitarie - elettorali	Ufficio tecnico	Si	Elettorale-giudiziari	si	Chiave

3.2.1.9. PERIFERICHE

PERIFERICHE		
Descrizione	Funzione	Attribuzione
Stampanti di rete	Stampa documenti degli utenti	Tutti gli utenti

3.2.1.10. STRUMENTI DI RETE

STRUMENTI DI RETE		
Descrizione	Funzione	Attribuzione
Schede Lan	Rete interna	Personale IT
Rete adsl	Rete collegamento a internet	Personale IT

3.2.1.11. STRUMENTI DI COMUNICAZIONE

STRUMENTI DI COMUNICAZIONE		
Descrizione	Funzione	Attribuzione
Router	Traffico dati RUPAR	IT

3.2.1.12. STRUMENTI DI SICUREZZA

STRUMENTI DI SICUREZZA			
Descrizione	Funzione	Aggiornamenti Annuali	
		Periodicità	Tipo

3.3. Analisi del livello di vulnerabilità

Come detto, il livello di vulnerabilità è stato analizzato valutando le misure di sicurezza implementate. Ciascun gruppo di contromisure è stato posto in relazione alle minacce rispetto alle quali le contromisure sono efficaci in termini di minimizzazione del rischio. In quest'ottica, la seguente tabella rappresenta le relazioni intercorrenti tra i gruppi di contromisure e le minacce da esse prevenute o limitate. Tali relazioni sono state utilizzate per effettuare l'analisi della vulnerabilità.

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza
Minacce informatiche	Scambio di credenziali di autenticazione tra colleghi	Formazione	-
		Policy e Procedure operative	-
		Individuazione per iscritto degli Incaricati	-
		Utilizzo di credenziali di autenticazione (user id+password)	x
		Utilizzo di credenziali di autenticazione (smart card-token)	-
		Utilizzo di credenziali di autenticazione (chiavi biometriche)	-
		Utilizzo di password con almeno 8 caratteri o massimo consentito dal sistema	-
		Modifica delle password ogni 3 mesi (nel caso di dati sensibili)	-
		Modifica delle password ogni 6 mesi (nel caso di dati personali)	-
		Codici identificativi (user id) univoci	-
		Codici identificativi (user id) non riassegnati in tempi successivi	-
		Disattivazione (non cancellazione) delle user id in caso di non utilizzo di almeno 6 mesi	-
	Accessi esterni non autorizzati	Sistemi a protezione di accessi abusivi (Firewall)	-
		Sistemi di intrusion detection	-
		Utilizzo di credenziali di autenticazione (smart card-token)	-
		Utilizzo di credenziali di autenticazione (chiavi biometriche)	-
		Utilizzo di credenziali di autenticazione (user id+password)	-
		Utilizzo di password con almeno 8 caratteri o massimo consentito dal sistema	-
		Modifica delle password ogni 3 mesi (nel caso di dati sensibili)	-
		Modifica delle password ogni 6 mesi (nel caso di dati personali)	-
		Codici identificativi (user id) univoci	-
		Codici identificativi (user id) non riassegnati in tempi successivi	-
		Disattivazione (non cancellazione) delle user id in caso di non	-

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza
		utilizzo di almeno 6 mesi	
		Sistemi di cifratura dati o supporti	-
		Aggiornamento programmi per elaboratore volti a prevenirne le vulnerabilità	-
		Verifiche periodiche dell'aggiornamento dei programmi per elaboratore	-
	Ricezione e azione di virus informatici	Software antivirus sugli elaboratori	x
		Software antivirus del sistema di posta elettronica	x
		Aggiornamento software antivirus	x
		Verifiche periodiche sui software antivirus	-
	Intercettazione di informazioni riservate	Utilizzo di password per l'apertura dei file	-
		Utilizzo di sistemi di crittografia	-
		Utilizzo di firma digitale	-
		Sistemi di intrusion detection	-
		Sistemi a protezione di accessi abusivi (Firewall)	-
	Incidenti, guasti, malfunzionamenti tecnici	Back Up e Verifica del Restore delle informazioni	x
		Procedure operative di business continuity	-
		Procedure operative di disaster recovery	-
		Manutenzione sistemi e impianti	-
		Piano di manutenzione	-
	Mancanza o fallimento di connessioni	Linee di comunicazione ridondanti	-
		Procedure operative di business continuity	-
Minacce naturali	Incendio	Sistemi antincendio manuali	x
		Sistemi antincendio automatici	x
		Manutenzione sistemi	x
		Formazione	-
		Distribuzioni di compiti e responsabilità ex D.Lgs. 626/94	-
		Back Up e Verifica del Restore delle informazioni	x
		Procedure operative di business continuity	-
		Procedure operative di disaster recovery	-
	Allagamento	Back Up e Verifica del Restore delle informazioni	x
		Sistemi antiallagamento automatici	-
		Manutenzione sistemi	-
		Procedure operative di business continuity	-
		Procedure operative di disaster recovery	-
	Disastri naturali	Back Up e Verifica del Restore delle informazioni	x
		Procedure operative di business continuity	-
		Procedure operative di disaster recovery	-
	Mancanza di energia elettrica	Back Up e Verifica del Restore delle informazioni	x
		Adegutezza dell'impianto elettrico alla destinazione d'utilizzo	x
		UPS (uninterruptible power supply)	x
		Generatori	-
	Mancanza di aria	Back Up e Verifica del Restore delle informazioni	x
		Adegutezza dell'impianto elettrico alla destinazione d'utilizzo	-

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza
	condizionata in locali critici (es. sala server)	UPS (uninterruptible power supply)	-
		Generatori	-
Minacce Umane	Accessi fisici non autorizzati	Servizio di reception	-
		Registrazione visitatori e consegna tesserini/badge "Visitatori"	-
		Sistema di controllo accessi	-
		Sistemi di Videosorveglianza	-
		Sistema di allarme	x
	Furto di dati da parte di personale interno	Back Up e Verifica del Restore delle informazioni	x
		Formazione	-
		Policy e Procedure operative	-
		Sistemi di cifratura dati o supporti	-
		Controlli su documenti, supporti e operazioni di eleborazione	-
		Custodia di atti, documenti e supporti removibili in armadi o cassettiere munite di serratura	-
		Registrazione degli accessi ad archivi contenenti dati sensibili dopo l'orario di lavoro	-
	Furto di dati da parte di terzi	Back Up e Verifica del Restore delle informazioni	x
		Sistema di controllo accessi	-
		Sistema di allarme	x
		Sistemi di Videosorveglianza	-
		Sistemi di cifratura dati o supporti	-
		Controlli su documenti, supporti e operazioni di eleborazione	-
		Custodia di atti, documenti e supporti removibili in armadi o cassettiere munite di serratura	-
		Registrazione degli accessi ad archivi contenenti dati sensibili dopo l'orario di lavoro	-
	Danneggiamento volontario di personale interno a beni aziendali	Back Up e Verifica del Restore delle informazioni	x
		Formazione	-
		Policy e Procedure operative	-
		Procedure operative di business continuity	-
		Procedure operative di disaster recovery	-
	Danneggiamento volontario di terzi soggetti a beni aziendali	Back Up e Verifica del Restore delle informazioni	x
		Sistema di identificazione e autenticazione degli accessi	-
		Sistema di allarme	x
		Sistemi di Videosorveglianza	-
		Controlli su documenti, supporti e operazioni di eleborazione	-
	Errori di manutenzione dei sistemi informativi	Back Up e Verifica del Restore delle informazioni	x
		Formazione	-
		Policy e Procedure operative	-
		Nomina d'Incarico di Amm. di Sistema	-
		Piano di manutenzione	-
		Attestazione di conformità del fornitore esterno	x
	Errori di utenti nelle	Back Up e Verifica del Restore delle informazioni	x
		Formazione	-

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza
	operazioni di elaborazione dei dati	Policy e Procedure operative	-
		Nomine d'Incarico al trattamento dei dati	x
		Controlli su documenti, supporti e operazioni di eleborazione	-
	Cattivo utilizzo di risorse di sistema	Formazione	-
		Policy e Procedure operative	-
		Controlli su documenti, supporti e operazioni di eleborazione	-
		Nomine d'Incarico al trattamento dei dati	x
	Uso non autorizzato di applicazioni	Formazione	-
		Policy e Procedure operative	-
		Nomine d'Incarico al trattamento dei dati	x
		Utilizzo di credenziali di autenticazione	x
		Profili di autorizzazione	x
		Autorizzazioni al trattamento dei dati sensibili	-
		Verifiche periodiche incarichi e profili di autorizzazione	-
		Registrazione degli accessi alle applicazioni	-
		Controlli su documenti, supporti e operazioni di eleborazione	-
		Distruzione e/o formattazione dei supporti removibili	0

3.4. Matrici di analisi dei rischi (sistema informativo complessivo)

3.4.1. Matrice di analisi dei rischi

ANNO 2004/2005	Evento	Probabilità di accadimento			Livello di Impatto sulla sicurezza (in termini di business, conseguenze legali e immagine)			Livello di Vulnerabilità	Individuazione quantitativa dell'esposizione al rischio	Individuazione qualitativa dell'esposizione al rischio	Percentuale di esposizione al rischio	Media Percentuale per categoria di minaccia
		Dato storico	Probabilità contestuale	Probabilità motivazionale	Riservatezza	Integrità	Disponibilità					
Minacce informatiche	Scambio di credenziali di autenticazione tra colleghi	1	1	1	5	4	3	4,7	24	Medio	18,9	20,7
	Accessi esterni non autorizzati	1	1	1	5	4	3	5,0	25	Medio	20,0	
	Ricezione e azione di virus informatici	3	3	3	5	5	5	1	15	Medio	12,0	
	Intercettazione di informazioni riservate	1	1	1	5	N/A	N/A	5,0	25	Medio	20,0	
	Incidenti, guasti, malfunzionamenti tecnici	3	1	1	3	4	4	3,7	25	Medio	19,7	
	Mancanza o fallimento di connessioni	3	1	1	N/A	2	5	5,0	42	Alto	33,3	
Minacce naturali	Incendio	1	1	1	N/A	5	5	2,5	13	Medio	10,0	18,8
	Allagamento	1	1	1	N/A	5	5	3,8	19	Medio	15,4	
	Disastri naturali	1	1	N/A	N/A	5	5	3,3	17	Medio	13,3	
	Mancanza di energia elettrica	5	5	1	N/A	3	3	1,4	16	Medio	12,6	
	Mancanza di aria condizionata in locali critici	5			N/A	3	3	3,6	54	Alto	42,9	
Minacce Umane	Accessi fisici non autorizzati	3	1	1	5	N/A	4	4,0	33	Medio	26,7	14,9
	Furto da parte di personale inerno	1	1	1	5	N/A	5	4,4	22	Medio	17,5	
	Furto da parte di terzi	1	1	1	5	N/A	5	3,8	19	Medio	15,2	
	Danneggiamento volontario di personale interno a beni aziendali	1	1	1	N/A	4	5	4,0	20	Medio	16,0	
	Danneggiamento volontario di terzi soggetti a beni aziendali	1	1	1	N/A	4	5	3,1	15	Medio	12,3	
	Errori di manutenzione ai sistemi informativi	1	1	1	4	4	4	3,6	14	Medio	11,4	
	Errori di utenti nelle operazioni di elaborazione dei dati	1	1	1	4	4	4	3,1	12	Medio	9,8	
	Cattivo utilizzo di risorse di sistema	1	1	1	4	4	4	3,6	15	Medio	11,6	
	Uso non autorizzato di applicazioni	1	1	1	5	5	4	3,3	16	Medio	13,1	

Esposizione grafica del livello percentuale di rischio

Le immagini seguenti mostrano rispettivamente l'esposizione percentuale al rischio di minacce informatiche (Figura 1), al rischio di minacce naturali (Figura 2) e al rischio di minacce umane (Figura 3).

L'ultima immagine (Figura 4) confronta, inoltre, le medie percentuali di esposizione al rischio per categoria di minaccia.

3.4.2. Esposizione grafica del livello di esposizione percentuale al rischio di Minacce Informatiche

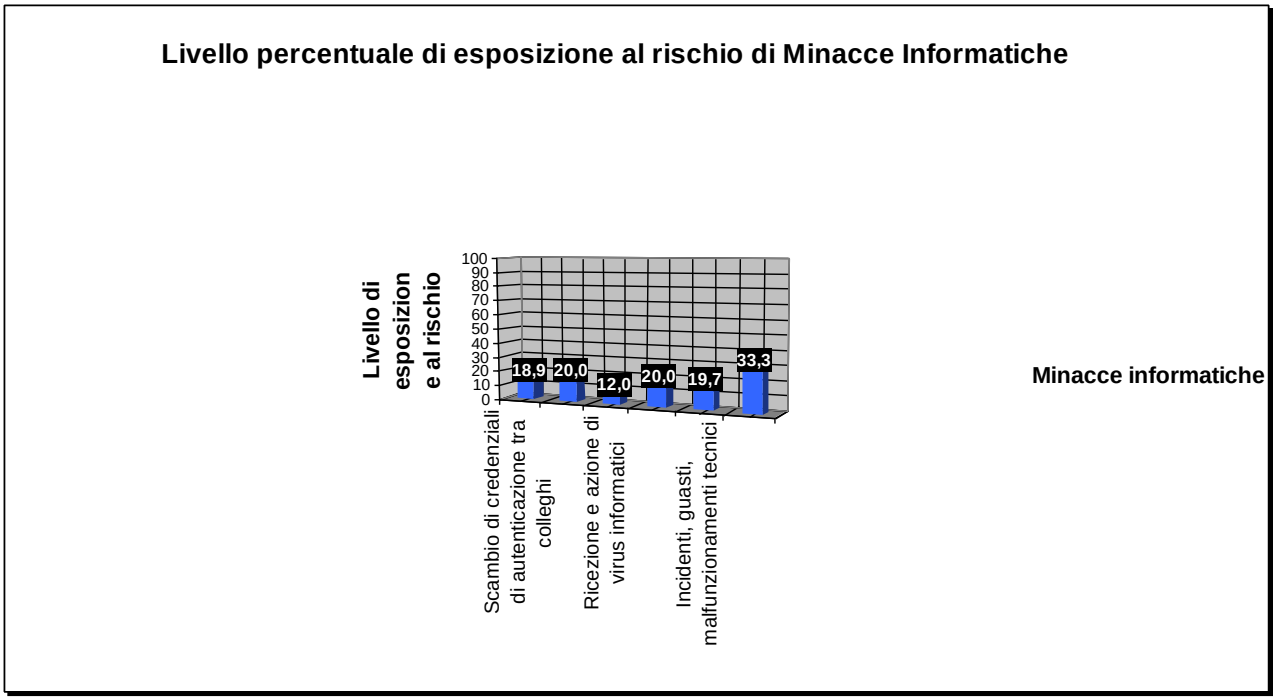


Figura 1

3.4.3. Esposizione grafica del livello di esposizione percentuale al rischio di Minacce Naturali

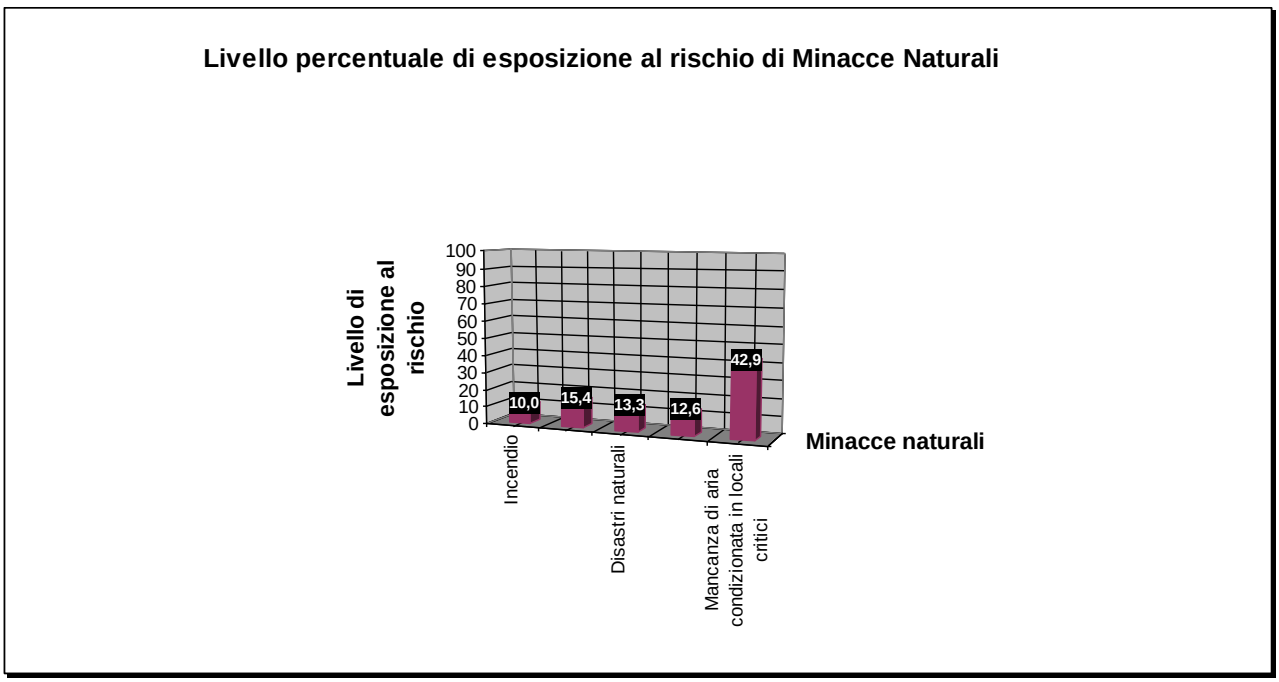


Figura 2

3.4.4. Esposizione grafica del livello di esposizione percentuale al rischio di Minacce Umane

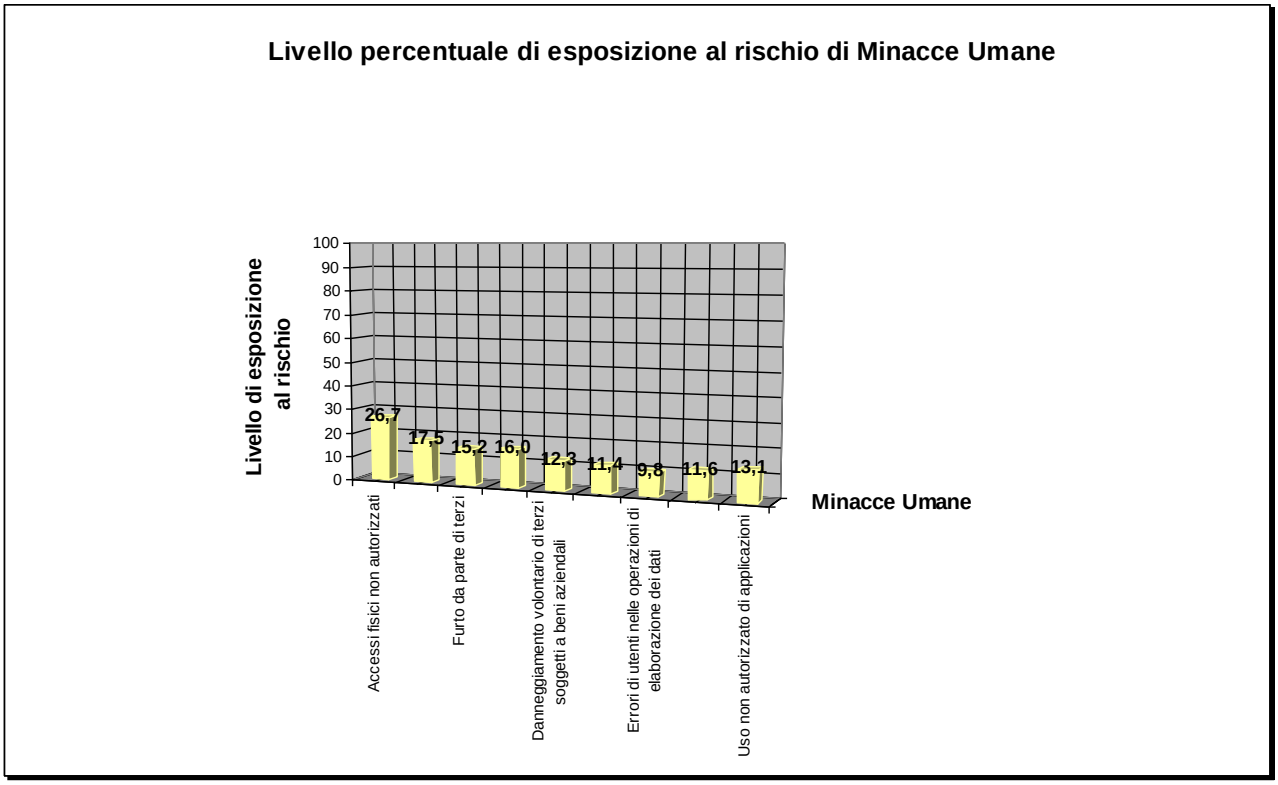


Figura 3

3.4.5. Confronto livello medio percentuale di esposizione al rischio per tipologia di minaccia

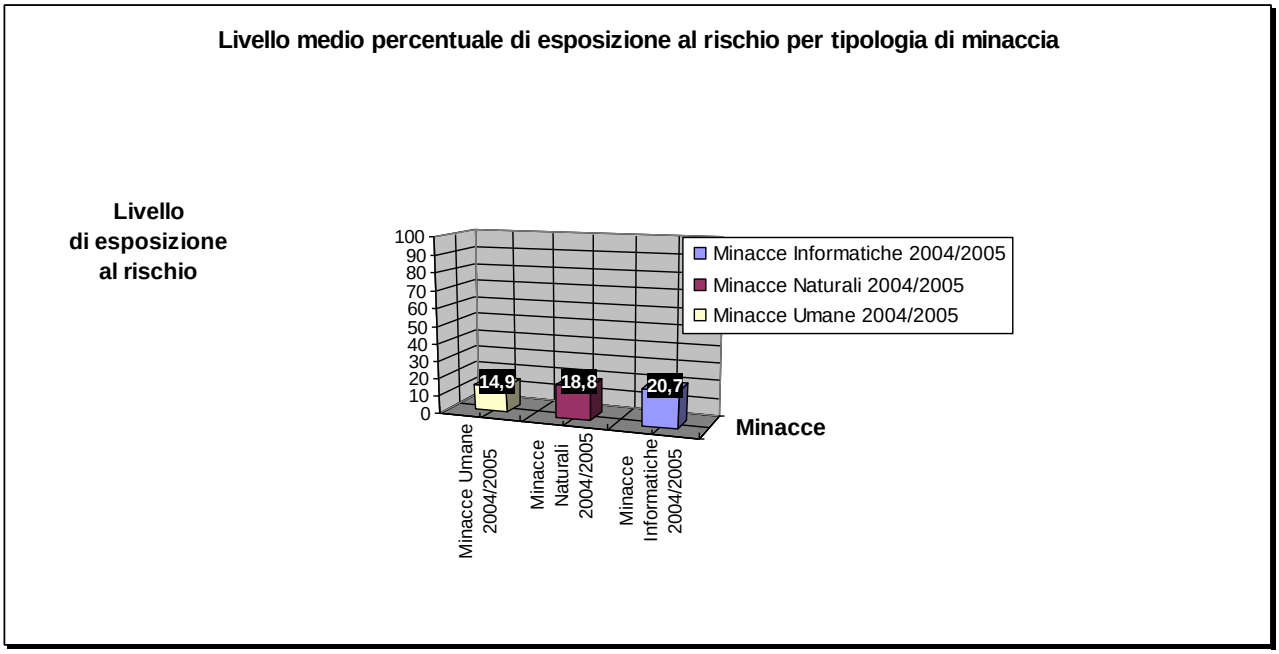


Figura 4

4. Misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Le seguenti tabelle indicano le misure di sicurezza adottate e quelle da adottare per conformarsi alle nuove misure minime di sicurezza.

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza DOPO
Minacce informatiche	Scambio di credenziali di autenticazione tra colleghi	Formazione	da implementare
		Policy e Procedure operative	da implementare
		Individuazione per iscritto degli Incaricati	da implementare
		Utilizzo di credenziali di autenticazione (user id+password)	già presente
		Utilizzo di credenziali di autenticazione (smart card-token)	
		Utilizzo di credenziali di autenticazione (chiavi biometriche)	
		Utilizzo di password con almeno 8 caratteri o massimo consentito dal sistema	da implementare
		Modifica delle password ogni 3 mesi (nel caso di dati sensibili)	da implementare
		Modifica delle password ogni 6 mesi (nel caso di dati personali)	da implementare
		Codici identificativi (user id) univoci	da implementare
		Codici identificativi (user id) non riassegnati in tempi successivi	da implementare
		Disattivazione (non cancellazione) delle user id in caso di non utilizzo di almeno 6 mesi	da implementare
	Accessi esterni non autorizzati	Sistemi a protezione di accessi abusivi (Firewall)	da implementare
		Sistemi di intrusion detection	
		Utilizzo di credenziali di autenticazione (smart card-token)	
		Utilizzo di credenziali di autenticazione (chiavi biometriche)	
		Utilizzo di credenziali di autenticazione (user id+password)	
		Utilizzo di password con almeno 8 caratteri o massimo consentito dal sistema	da implementare
		Modifica delle password ogni 3 mesi (nel caso di dati sensibili)	da implementare
		Modifica delle password ogni 6 mesi (nel caso di dati personali)	da implementare
		Codici identificativi (user id) univoci	da implementare
		Codici identificativi (user id) non riassegnati in tempi successivi	da implementare
		Disattivazione (non cancellazione) delle user id in caso di non utilizzo di almeno 6 mesi	da implementare
		Sistemi di cifratura dati o supporti	
		Aggiornamento programmi per elaboratore volti a prevenirne le vulnerabilità	da implementare
		Verifiche periodiche dell'aggiornamento dei programmi per	da

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza DOPO
		elaboratore	implementare
	Ricezione e azione di virus informatici	Software antivirus sugli elaboratori	già presente
		Software antivirus del sistema di posta elettronica	già presente
		Aggiornamento software antivirus	già presente
		Verifiche periodiche sui software antivirus	da implementare
	Intercettazione di informazioni riservate	Utilizzo di password per l'apertura dei file	
		Utilizzo di sistemi di crittografia	
		Utilizzo di firma digitale	
		Sistemi di intrusion detection	
		Sistemi a protezione di accessi abusivi (Firewall)	da implementare
	Incidenti, guasti, malfunzionamenti tecnici	Back Up e Verifica del Restore delle informazioni	già presente
		Procedure operative di business continuity	
		Procedure operative di disaster recovery	
		Manutenzione sistemi e impianti	
		Piano di manutenzione	
	Mancanza o fallimento di connessioni	Linee di comunicazione ridondanti	
		Procedure operative di business continuity	0
Minacce naturali	Incendio	Sistemi antincendio manuali	
		Sistemi antincendio automatici	
		Manutenzione sistemi	
		Formazione	
		Distribuzioni di compiti e responsabilità ex D.Lgs. 626/94	da implementare
		Back Up e Verifica del Restore delle informazioni	già presente
		Procedure operative di business continuity	0
		Procedure operative di disaster recovery	0
	Allagamento	Back Up e Verifica del Restore delle informazioni	già presente
		Sistemi antiallagamento automatici	
		Manutenzione sistemi	x
		Procedure operative di business continuity	0
		Procedure operative di disaster recovery	0
	Disastri naturali	Back Up e Verifica del Restore delle informazioni	già presente
		Procedure operative di business continuity	0
		Procedure operative di disaster recovery	0
	Mancanza di energia elettrica	Back Up e Verifica del Restore delle informazioni	già presente
		Adeguatezza dell'impianto elettrico alla destinazione d'utilizzo	x
		UPS (uninterruptible power supply)	
		Generatori	
	Mancanza di aria condizionata in locali critici (es. sala server)	Back Up e Verifica del Restore delle informazioni	già presente
		Adeguatezza dell'impianto elettrico alla destinazione d'utilizzo	x
		UPS (uninterruptible power supply)	0
		Generatori	0
Minacce	Accessi fisici	Servizio di reception	

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza DOPO
Umane	non autorizzati	Registrazione visitatori e consegna tesserini/badge "Visitatori"	
		Sistema di controllo accessi	
		Sistemi di Videosorveglianza	
		Sistema di allarme	
	Furto di dati da parte di personale interno	Back Up e Verifica del Restore delle informazioni	già presente
		Formazione	
		Policy e Procedure operative	
		Sistemi di cifratura dati o supporti	
		Controlli su documenti, supporti e operazioni di eleborazione	
		Custodia di atti, documenti e supporti removibili in armadi o cassettiere munite di serratura	da implementare
		Registrazione degli accessi ad archivi contenenti dati sensibili dopo l'orario di lavoro	
	Furto di dati da parte di terzi	Back Up e Verifica del Restore delle informazioni	già presente
		Sistema di controllo accessi	0
		Sistema di allarme	0
		Sistemi di Videosorveglianza	0
		Sistemi di cifratura dati o supporti	0
		Controlli su documenti, supporti e operazioni di eleborazione	0
		Custodia di atti, documenti e supporti removibili in armadi o cassettiere munite di serratura	da implementare
		Registrazione degli accessi ad archivi contenenti dati sensibili dopo l'orario di lavoro	0
	Danneggiamento volontario di personale interno a beni aziendali	Back Up e Verifica del Restore delle informazioni	già presente
		Formazione	0
		Policy e Procedure operative	0
		Procedure operative di business continuity	0
		Procedure operative di disaster recovery	0
	Danneggiamento volontario di terzi soggetti a beni aziendali	Back Up e Verifica del Restore delle informazioni	già presente
		Sistema di identificazione e autenticazione degli accessi	0
		Sistema di allarme	0
		Sistemi di Videosorveglianza	0
		Controlli su documenti, supporti e operazioni di eleborazione	0
	Errori di manutenzione dei sistemi informativi	Back Up e Verifica del Restore delle informazioni	già presente
		Formazione	0
		Policy e Procedure operative	0
		Nomina d'Incarico di Amm. di Sistema	
		Piano di manutenzione	
		Attestazione di conformità del fornitore esterno	
	Errori di utenti nelle operazioni di elaborazione dei dati	Back Up e Verifica del Restore delle informazioni	già presente
		Formazione	0
		Policy e Procedure operative	0
		Nomine d'Incarico al trattamento dei dati	x
		Controlli su documenti, supporti e operazioni di eleborazione	0
	Cattivo utilizzo	Formazione	0

	EVENTO	MISURE DI SICUREZZA PER LA RIDUZIONE DEL RISCHIO	Presenza misure di sicurezza DOPO
	di risorse di sistema	Policy e Procedure operative	0
		Controlli su documenti, supporti e operazioni di eleborazione	0
		Nomine d'Incarico al trattamento dei dati	x
	Uso non autorizzato di applicazioni	Formazione	0
		Policy e Procedure operative	0
		Nomine d'Incarico al trattamento dei dati	x
		Utilizzo di credenziali di autenticazione	già presente
		Profili di autorizzazione	già presente
		Autorizzazioni al trattamento dei dati sensibili	N/A
		Verifiche periodiche incarichi e profili di autorizzazione	da implementare
		Registrazione degli accessi alle applicazioni	
		Controlli su documenti, supporti e operazioni di eleborazione	0
		Distruzione e/o formattazione dei supporti removibili	da implementare

5. Linee Guida in fase di formalizzazione per garantire il rispetto delle misure minime di sicurezza e la sicurezza dei dati personali

Nel presente capitolo si riportano le Linee Guida predisposte dall'organizzazione che verranno formalizzate entro i termini di legge al fine di conformarsi rispetto alla normativa in materia di protezione dei dati personali.

5.1. Linee Guida per la sicurezza nel trattamento dei dati personali

LINEE GUIDA PER LA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI	
1	Utilizzo delle chiavi ed accesso agli uffici e agli archivi
2	Conservazione dei supporti (CD Rom, dischetti, copie cartacee, fascicoli, ecc.) in un luogo sicuro
3	Utilizzo di Stampanti, Fotocopiatrici e Fax
4	Fasi del trattamento di dati personali
5	Le chiavi di accesso ai dati informatici, in particolare le password
5.1	Custodia delle password
5.2	Regole inerenti le password
5.3	COSA NON FARE
5.4	COSA FARE
5.5	Come scegliere una password
6	Traccia dei dati riservati
7	Utilizzo di elaboratori portatili
8	Divieto di utilizzo del computer da parte di personale esterno
9	Divieto di installazione e utilizzazione di apparecchi non autorizzati
10	Divieto di utilizzazione di programmi non autorizzati
11	Linee guida per la prevenzione delle infezioni da Virus
11.1	Come si trasmettono i virus degli elaboratori
11.2	Quando il rischio è alto
11.3	Effetti dei virus
11.4	Come prevenire i virus
11.4.1	Utilizzare soltanto programmi installati dall'Amministratore di Sistema

11.4.2	Assicurarsi di non far partire accidentalmente il Vostro computer da dischetto
11.4.3	Proteggere i dischetti da scrittura (quando possibile)
11.4.4	Utilizzo di Software antivirus aggiornati
12	Politica locale relativa ai back-up

5.2. Linee Guida per Amministratore di Sistema e Gestore Password

LINEE GUIDA PER AMMINISTRATORE DI SISTEMA E GESTORE PASSWORD	
1	Nomina degli Amministratori di sistema e custodi o gestori delle password
2	Credenziali di Autenticazione
3	Parole Chiave (password)
4	Codici Identificativi
5	Disattivazione delle credenziali
6	Sistema e profili di autorizzazione
7	Sistemi di sicurezza e antivirus
8	Aggiornamenti periodici programmi per elaboratore
9	Back-up e ripristino dei dati
10	Supporti rimuovibili e dismissione elaboratori
11	Affidamento a terzi per implementazione di misure minime di scurezza
12	Controlli periodici, analisi dei rischi e documento programmatico sulla sicurezza
13	Elaboratori destinati ad accessi da parte di più incaricati/utenti

5.3. Linee Guida per il trattamento dei dati del Personale

LINEE GUIDA PER IL TRATTAMENTO DEI DATI DEL PERSONALE	
1	Rispetto della vita privata e della dignità umana dei lavoratori
2	Informazione e consultazione dei lavoratori
3	Raccolta dei dati
4	Registrazione dei dati
5	Utilizzazione interna dei dati
6	Comunicazione di dati ai rappresentanti dei lavoratori
7	Comunicazione di dati all'esterno
8	Categorie particolari di dati
9	Diritti di accesso e di rettifica
10	Conservazione dei dati

5.4. Linee Guida per l'utilizzo della Posta Elettronica e di Internet

LINEE GUIDA PER L'UTILIZZO DELLA POSTA ELETTRONICA E DI INTERNET	
1	Uso lavorativo degli strumenti dell'organizzazione
2	Controlli ed ispezioni dell'organizzazione nel rispetto dell'art. 4 dello Statuto dei lavoratori
3	Divieti nell'utilizzo di tali strumenti
4	Rischi di sicurezza nell'utilizzo scorretto o abusivo di tali strumenti
5	Sanzioni in caso di abuso di tali strumenti

6. Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Conformemente all'articolo 19.5. del Disciplinare Tecnico in materia di misure minime di sicurezza il presente paragrafo riporta la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

L'Ente sta implementando specifiche procedure operative per garantire un sistema di ripristino dei dati in tempi utili per il rispetto dei diritti degli interessati e, comunque, entro 7 giorni dalla data dell'incidente.

7. Piano di Formazione

Il piano di formazione prevedrà interventi formativi per tutti gli incaricati del trattamento, al fine di renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dall'Ente.

La seguente tabella riporta le informazioni concernenti le sessioni formative pianificate:

PERSONALE	TIPOLOGIA FORMAZIONE	PERIODICITÀ	DURATA	TERMINE
Incaricati	Manualistica	Continuativa	Continuativa	Entro termine di legge

Il processo formativo, inoltre, sarà programmato già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

8. Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare

Conformemente all'articolo 19.7. del Disciplinare Tecnico in materia di misure minime di sicurezza il presente paragrafo riporta la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

In base alle nuove policy, che saranno introdotte entro i termini di legge, nel caso di affidamento a terzi di trattamenti in outsourcing la garanzia del rispetto delle misure minime di sicurezza da parte del fornitore sarà affidata a specifiche clausole contrattuali. A seconda dei casi, in base alle procedure operative in materia, il soggetto fornitore sarà nominato responsabile del trattamento (in caso di impresa) affinché – attraverso il mansionario di nomina – si precisino gli impegni alla riservatezza e alla protezione dei dati. Tale nomina non sarà di regola effettuata nei confronti dei soggetti iscritti ad Albi professionali (Consulenti del lavoro, Avvocati, Commercialisti, Medici) che abbiano un codice deontologico ad ulteriore garanzia.

I terzi soggetti preposti ai trattamenti di dati personali sono indicati nei paragrafi di cui al capitolo 1.

9. Criteri da adottare per la cifratura o per la separazione dagli altri dati personali dell'interessato dei dati personali idonei a rivelare lo stato di salute e la vita sessuale

Le disposizioni dell'articolo 19.8. del Disciplinare Tecnico in materia di misure minime di sicurezza si applicano esclusivamente agli organismi sanitari e agli esercenti professioni sanitarie, come ricordato dall'Autorità Garante per la protezione dei dati personale nel modello pubblicato di Documento Programmatico sulla Sicurezza. Pertanto, tale misura di sicurezza non è applicabile alla realtà del Comune di Grignasco.

COMUNE DI GRIGNASCO

ALLEGATO 11

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Amministrazione e tutti i documenti informatici.

Sono escluse dalla protocollazione, ai sensi dell'art. 53 c. 5 del DPR 445/2000 le seguenti tipologie documentarie:

- Gazzette ufficiali, Bollettini ufficiali PA;
- Notiziari PA;
- Giornali, riviste, libri;
- Materiali pubblicitari;
- Note di ricezione altre disposizioni;
- 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…);
- Documentazione già soggetta, direttamente od indirettamente, a registrazione particolare (es. vaglia, assegni, ecc…)

Vengono altresì esclusi dall'obbligo di protocollazione i seguenti documenti cartacei/digitali interni:

- Richieste ferie;
- Richieste permessi;
- Verbali di gara;
- Ricevute di ritorno delle raccomandate A.R.;
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura;

Vengono altresì esclusi dall'obbligo di protocollazione i seguenti documenti cartacei/digitali esterni:

- Pubblicità conoscitiva di convegni;
- Pubblicità generale;
- Offerte e listini prezzi

Comune di Grignasco Data di stampa
Stampa Tabella Classi
24/12/2015
Codice Descrizione
Categoria I Amministrazione generale
1 Legislazione e circolari esplicative
2 Denominazione, territorio e confini, circoscrizioni 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 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 per l'esercizio di funzioni e servizi
16 Area e città metropolitana
17 Associazionismo e partecipazione

Comune di Grignasco Data di stampa
Stampa Tabella Classi
24/12/2015
Codice Descrizione
Categoria II Organi di governo, gestione, controllo, consulenza
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
22 Conferenza dei Presidenti di quartiere

Comune di Grignasco Data di stampa
Stampa Tabella Classi
24/12/2015
Codice Descrizione
Categoria 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 Adempimenti fiscali, contributivi e assicurativi
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

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria IV Risorse finanziarie e patrimonio
1 Entrate
2 Uscite
3 Partecipazioni finanziarie
4 Bilancio preventivo, variazioni di bilancio, verifiche contabili
5 Piano esecutivo di gestione (PEG)
6 Rendiconto della gestione
7 Adempimenti fiscali
8 Inventari e consegnatari dei beni
9 Beni immobili
10 Beni mobili
11 Economato
12 Oggetti smarriti e recuperati
13 Tesoreria
14 Concessionari ed altri incaricati della riscossione delle entrate
15 Pubblicità e pubbliche affissioni

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria V Affari legali
1 Contenzioso
2 Responsabilità civile e patrimoniale verso terzi; assicurazioni
3 Pareri e consulenze

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria 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, luce, gas, trasporti pubblici, gestione rifiuti e altri servizi
9 Ambiente: autorizzazioni, monitoraggio e controllo
10 Protezione civile ed emergenze

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria 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, privati e volontariato
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

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria 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

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria IX Polizia locale e sicurezza pubblica
1 Prevenzione ed educazione stradale
2 Polizia stradale
3 Informative
4 Sicurezza e ordine pubblico

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria X Tutela della salute
1 Salute e igiene pubblica
2 Trattamento Sanitario Obbligatorio
3 Farmacie
4 Zooprofilassi veterinaria
5 Randagismo animale e ricoveri

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria XI Servizi demografici
1 Stato civile
2 Anagrafe e certificazioni
3 Censimenti
4 Polizia mortuaria e cimiteri

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria XII Elezioni ed iniziative popolari
1 Albi elettorali
2 Liste elettorali
3 Elezioni
4 Referendum
5 Istanze, petizioni e iniziative popolari

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria XIII Leva militare
1 Leva
2 Ruoli Matricolari
3 Caserme, alloggi e servitù militari
4 Requisizioni per utilità militari

Comune di Grignasco Data di stampa

Stampa Tabella Classi

24/12/2015
Codice Descrizione
Categoria XIV Oggetti diversi