?

Stampa

COMUNE DI GATTEO

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO E DELLA GESTIONE DEI FLUSSI DOCUMENTALI E CONSERVAZIONE DEI DOCUMENTI

INDICE

ALLEGATI

INTRODUZIONE

Il Comune di Gatteo ha sostituito nel 2003 il sistema precedentemente in uso per il protocollo e la gestione degli atti, adottando un nuovo sistema di "gestione documentale" - inteso come sistema di gestione informatica dei documenti in modalità avanzata - denominato **"Protocollo ed Atti",** la cui utilizzazione ha richiesto e richiederà ancora nei prossimi mesi una analisi organizzativa e successiva personalizzazione ed integrazione con il sistema informativo esistente e con altre funzioni previste da altre normative (es. la firma digitale e la gestione documentale elettronica).
Trattandosi di un sistema modulare, Protocollo ed Atti consente di gestire separatamente e/o contestualmente, oltre ai dati necessari alla tenuta del registro di protocollo, altre informazioni e funzioni più evolute, riferite alle funzionalità proprie del patrimonio informativo dell'Amministrazione (Creazione e gestione degli atti, collegamenti con le Banche dati inerenti la struttura organizzativa ed i corrispondenti esterni dell'Amministrazione, Gestione dei procedimenti amministrativi).
L'Amministrazione Comunale ha inoltre aderito al progetto "Panta Rei", avente la finalità di costruire un network territoriale a scala Provinciale tra le Amministrazioni pubbliche per la circolazione digitale della documentazione amministrativa, attraverso la realizzazione di un Sistema Centrale di archiviazione dei documenti protocollati e l'integrazione degli applicativi del protocollo con una piattaforma di gestione documentale. Si ritiene che entro il 2004 tutti gli Enti aderenti saranno dotati degli strumenti necessari per consentire la circolazione digitale delle informazioni nel rispetto delle vigenti normative. La ditta che ha elaborato "Protocollo ed Atti" rientra tra quelle che hanno avviato la procedura di accreditamento al Progetto, garantendo l'adeguamento del software alle norme Aipa ed alle specifiche progettuali Panta Rei in materia di gestione informatica dei documenti. Il sistema di gestione documentale adottato consentirà pertanto nell'immediato futuro la gestione a norma di legge della documentazione elettronica, l'introduzione della firma digitale e di una casella di posta certificata, l'archiviazione digitale dei documenti, la cooperazione ed interoperabilità del sistema con quelli delle altre amministrazioni pubbliche.

In questa fase di avvio del nuovo sistema di gestione documentale, si è inteso privilegiare l'utilizzazione del modulo del protocollo, introducendone l'uso in tutti i Settori del Comune. Tale innovazione, che ha già comportato un diverso modo di svolgere il lavoro amministrativo e di gestire la documentazione, si accompagna alle innovazioni introdotte dalla normativa che hanno avuto, e avranno anche in futuro, notevoli ricadute nella prassi amministrativa e gestionale.

Per questo motivo, e per disporre delle informazioni necessarie da un lato a gestire correttamente i flussi documentali, sia su supporto cartaceo sia su supporto informatico, e dall'altro a coordinarli, ed eventualmente a correggerli e modificarli, le Regole tecniche sul protocollo informatico (DPCM 31 ottobre 2000) prescrivono che ciascuna pubblica amministrazione adotti un proprio *Manuale di gestione*.

Tale strumento "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio", comprendendo, tra l'altro, tutte le indicazioni per l'utilizzo dei documenti informatici (formazione, autenticazione, protocollazione, trasmissione, conservazione, sicurezza), la descrizione dei flussi di lavorazione dei documenti, il titolario di classificazione, le modalità di produzione e conservazione delle registrazioni di protocollo, la descrizione funzionale e operativa del sistema di protocollo informatico, i criteri e le modalità per le abilitazioni all'accesso ecc.

Si tratta indubbiamente di uno strumento complesso, che in alcune parti deve necessariamente subire aggiornamenti frequenti, ma che costituisce un punto di riferimento insostituibile per chiunque operi all'interno dell'Ente o abbia scambi documentali con esso.

In considerazione della attuale modalità di utilizzazione del sistema di gestione documentale da parte degli Uffici Comunali, nel manuale non sono state inseriti riferimenti alla firma elettronica o digitale dei documenti né all'archiviazione ottica, in quanto ancora non trovano applicazione nella pratica dell'ente. Si è comunque ritenuto opportuno predisporre un Allegato al Manuale, esplicativo dei principali contenuti del Progetto Panta Rei, contenente le informazioni al momento disponibili sugli standard tecnologici del progetto e sulle modalità attuative dello stesso, che sono strettamente rispondenti ai requisiti previsti dalla normativa.

Eventuali difformità che dovessero determinarsi, rispetto al contenuto del manuale, dall'introduzione di tali nuove metodologie di gestione, circolazione e conservazione della documentazione amministrativa, saranno immediatamente recepite.

L'operatore che abitualmente utilizza il software di gestione atti in dotazione agli uffici comunali, riconoscerà immediatamente la gestione di flussi documentali che corrisponde alla prassi attualmente in uso, mentre per le innovazioni introdotte si assicura che saranno preventivamente illustrate e sperimentate e, qualora condivise negli aspetti operativi, successivamente stabilmente introdotte.

SEZIONE I – PRINCIPI GENERALI

Articolo 1 – Struttura del Manuale

Il manuale di gestione è composto dai seguenti documenti:
1. Manuale di gestione e conservazione dei documenti (questo manuale)
2. Allegato 1 : Titolario di Classificazione
3. Allegato 2: Organigramma del Comune
4. Allegato 3: Documenti da non protocollare
5. Allegato 4: funzionalità del Sistema di gestione documentale e conformità normativa AIPA
6. Allegato 5: Piano della Sicurezza Informatica
7. Allegato 6: Abilitazione all'utilizzo del Sistema di gestione informatica dei documenti, livelli di riservatezza e corrispondenti logiche di protezione
8. Allegato 7: Presentazione del Progetto Panta Rei

Articolo 2 - Individuazione dell'area organizzativa omogenea

Il Testo unico delle disposizioni in materia di documentazione amministrativa (DPR 445 del 28 dicembre 2000) prescrive, all'art. 50, c.3, che ciascuna pubblica amministrazione individui, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e di archiviazione.
Il Comune di Gatteo ha sempre avuto un unico protocollo generale, che ha protocollato tutti i documenti in arrivo e in partenza dall'Ente.
A partire dal 1 settembre 2003 si è adottata una procedura per il protocollo informatico che può essere utilizzata da più stazioni contemporaneamente. Si è quindi iniziato partendo dal Settore Affari generali, seguito subito dopo dagli altri settori, un percorso di distribuzione della procedura del protocollo informatico per la registrazione della documentazione in partenza. Al momento tutti i Settori dispongono di almeno una stazione abilitata alla protocollazione.
In tale situazione, l'area organizzativa omogenea per la gestione coordinata dei documenti non poteva che coincidere con l'amministrazione comunale nel suo complesso, ed è per questo motivo che la Giunta Comunale con la deliberazione di approvazione del presente manuale individua all'interno dell'Ente un'unica area organizzativa omogenea.
Il Comune di Gatteo, pertanto, utilizza un unico sistema di protocollazione e un unico titolario di classificazione, e produce un unico archivio, in cui l'articolazione in archivio corrente, archivio di deposito e archivio storico rappresenta una mera suddivisione funzionale.

Articolo 3 - Definizioni

Ai fini del presente manuale si intende

a) per Amministrazione, Comune di Gatteo;
b) per area organizzativa omogenea, un insieme di funzioni e di strutture, individuate dall'Amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato;
c) per responsabile, quando non meglio specificato, il responsabile della tenuta del protocollo informatico , della gestione dei flussi documentali e degli archivi, individuato nel responsabile degli affari generali;
d) per documento amministrativo, ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque utilizzati ai fini dell'attività amministrativa;
e) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
f) per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
g) per impronta di un documento informatico, una sequenza di simboli binari in grado di identificarne univocamente il contenuto;
h) per gestione dei documenti, l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione adottato;
i) per sistema di gestione informatica dei documenti, l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti;
j) per segnatura di protocollo, l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
k) per archivio corrente, la parte di documentazione relativa ad affari ed ai procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse attuale;
l) per archivio di deposito, la parte di documentazione relativa ad affari esauriti, non più occorrenti alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente ed alla consultazione da parte del pubblico;
m) per archivio storico, il complesso di documenti relativi ad affari esauriti e destinati, previe operazioni di scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico, come previsto dal T.U. 490/1999;
n) per titolario di classificazione, un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la conservazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta;
o) per fascicolo, l'unità archivistica indivisibile di base che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare;
p) per classificazione, l'operazione che consente di organizzare i documenti in relazione alle funzioni ed alle modalità operative dell'Amministrazione, in base al titolario di classificazione;
q) per fascicolazione, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;
r) per assegnazione, l'operazione di individuazione del servizio utente competente per la trattazione del procedimento amministrativo o affare cui i documenti si riferiscono;

s) per documento analogico si intende un documento amministrativo prodotto su supporto non informatico. Di norma il documento analogico è un documento cartaceo.
t) per versione analogica di un documento informatico si intende una copia, di norma cartacea, di un documento prodotto in origine su supporto informatico.
u) per registro si intende un documento amministrativo costituito dalla registrazione in sequenza, secondo criteri predefiniti (tendenzialmente cronologici), in un unica entità documentaria di una pluralità di atti giuridici. In ambiente digitale i registri possono assumere la forma di database.
v) per serie si intende un raggruppamento, dettato da esigenze funzionali, di documenti con caratteristiche omogenee in relazione alla natura e alla forma dei documenti (serie delle determinazioni, dei contratti, dei registri di protocollo), o in relazione all'oggetto e alla materia (serie dei fascicoli personali, delle pratiche edilizie, ecc.).
w) per servizio utente, un servizio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti;
x) per testo unico, il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, pubblicato con DPR 28 dicembre 2000, n° 445.

SEZIONE II - TIPOLOGIE DI DOCUMENTI E REGIME GIURIDICO

Articolo 4 - Documento informatico

La produzione, trasmissione, gestione e conservazione di documenti informatici presentano caratteristiche e problematiche proprie rispetto ai documenti analogici, in particolare per gli aspetti relativi all'autenticità, affidabilità, stabilità. Considerando l'attuale dotazione dell'Ente, in termini di procedure ed attrezzature, e la perdurante preponderanza dei documenti analogici rispetto a quelli informatici, si ritiene preferibile, per il momento, produrre una versione analogica di ogni documento informatico prodotto o ricevuto dal Comune, in modo da poter gestire più agevolmente fascicoli e procedimenti che, diversamente, risulterebbero ibridi, composti da documenti sia cartacei che informatici. L'attuale situazione deve comunque essere considerata di transizione verso un uso più diffuso e generalizzato dei documenti informatici e delle versioni informatiche dei documenti analogici.

Articolo 5 - Documento analogico

Ogni documento cartaceo prodotto dal Comune di Gatteo va di norma redatto almeno in due esemplari, cioè in originale e in minuta. Per originale si intende il documento nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali (carta intestata, firma ecc.), comprendente tutti gli elementi di garanzia e di informazione di cui all'art.13. Per minuta si intende una copia dell'originale del documento conservato "agli atti", cioè nel fascicolo relativo all'affare o al procedimento amministrativo trattato. Sia l'originale che la copia vanno corredati di firma autografa e di timbro tondo dell'ufficio.

Articolo 6 – Regime giuridico

A norma dell'art. 2, c. 1 lett. d) e c. 4, e dell'art. 54 del D. lgs. 29 ottobre 1999, n. 490 (*Testo unico delle disposizioni legislative in materia di beni culturali e ambientali*), tutti i documenti del Comune di Gatteo (analogici ed informatici, ricevuti, spediti o interni) dal momento del loro inserimento nell'archivio del Comune mediante l'attribuzione di un codice di classificazione sono parte del demanio archivistico del Comune e come tali sono assoggettati al regime proprio del demanio pubblico. In quanto beni culturali fin dall'origine, i singoli documenti del Comune e l'archivio comunale nel suo complesso sono sottoposti a particolari tutele e garanzie: a norma degli art. 21 e 22 del D. lsg. 490/1999, è necessario richiedere l'autorizzazione della Soprintendenza archivistica per lo spostamento di fondi dell'archivio di deposito e dell'archivio storico, e per lo scarto di documentazione archivistica; inoltre, qualora abusivamente sottratti al Comune, i documenti del suo archivio sono rivendicabili senza limiti di tempo, purché si disponga di elementi che ne provino l'appartenenza (numeri di protocollo, indici di classificazione, descrizioni in inventari ecc.).

Articolo 7 - Tipologia dei Documenti

Considerando i documenti in relazione al modo in cui diventano parte integrante del sistema documentario del Comune, si può distinguere tra documenti in arrivo, documenti in partenza e documenti interni.

1. Per **documenti in arrivo** si intendono i documenti acquisiti dal Comune di Gatteo nell'esercizio delle proprie funzioni.
2. Per **documenti in partenza** si intendono i documenti prodotti nell'esercizio delle proprie funzioni dagli organi e dal personale in servizio presso il Comune.

3. Per **documenti interni** si intendono i documenti scambiati tra i Settori e Servizi del Comune, o tra uffici appartenenti ad un medesimo Settore o Servizio.
Questi ultimi si distinguono in :
1. Documenti di carattere informativo (spesso equivalenti ad una comunicazione verbale);
2. Documenti di preminente carattere giuridico – probatorio.

I documenti interni di carattere informativo sono memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra uffici e di norma non vanno protocollati.

I documenti interni di preminente carattere giuridico – probatorio sono quelli redatti dal personale dipendente dal Comune nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti l'attività amministrativa svolta , o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, e come tali devono essere protocollati.

L'operazione di protocollazione dei documenti interni in partenza è effettuata dal Responsabile del procedimento amministrativo o da un suo delegato.

Considerando invece il supporto e le modalità di formazione dei documenti, si possono identificare i casi seguenti:

1. **Documenti analogici**, prodotti con strumenti analogici (es.: lettera scritta a mano o a macchina) o con strumenti informatici (es.: lettera prodotta tramite un sistema di videoscrittura - Word ecc. - e stampata: come originale si considera quello cartaceo dotato di firma autografa ed eventualmente stampato su carta intestata): l'originale è analogico;

2. **Documenti informatici** (**file**) prodotti con strumenti informatici (ad es. file prodotti con strumenti come Word, Excel, Outlook, Notepad o qualunque altro editor ASCII); l'originale è informatico.

3. **Sistemi informatici:** documenti informatici costituiti dall'insieme di una procedura informatica e di una base dati gestite tramite dispositivi di elaborazione elettronica digitale (es. il protocollo informatico).

Articolo 8 - Casistica e modalità operative

Appare utile, dopo aver definito e individuato diverse tipologie di documenti, segnalare quali casi si presentano più frequentemente nella prassi amministrativa attuale e quali sono le specifiche modalità di gestione. Va sottolineato, a questo proposito, il ruolo strategico del responsabile del procedimento amministrativo individuato ai sensi della L. 241/1990, cui spettano scelte e valutazioni di primaria importanza.

Articolo 9 - Documenti in arrivo

Per quanto riguarda i **documenti in arrivo**, essi possono essere o documenti analogici, o file pervenuti via posta elettronica. Il Comune di Gatteo si riserva di trattare tutti i documenti informatici (pervenuti via posta elettronica) che l'attuale – e, soprattutto, del prossimo futuro - dotazione tecnologica ci permette di leggere e decodificare.

Articolo 10 - Documenti interni

I documenti interni al Comune possono essere analogici, o file o sistemi informatici. Per quanto riguarda questi ultimi, la scelta di utilizzare tecnologie informatiche per la gestione, ad esempio, del

protocollo o degli atti e documenti implica necessariamente l'utilizzo e la conseguente validità di documenti informatici complessi costituiti dall'insieme di una base dati e di una procedura che la gestisce. La scelta di ricorrere a documenti analogici o a file nell'ambito di un procedimento amministrativo spetta unicamente al responsabile del procedimento, dal momento che tale materia non è ancora stata disciplinata dal regolamento dei procedimenti amministrativi del Comune di Gatteo.

Articolo 11 - Documenti in partenza

I **documenti in partenza**, prodotti dal Comune e destinati all'esterno, possono essere analogici o informatici (file) **e sistemi informatici;** anche in questo caso, in mancanza di una specifica regolamentazione, spetta al responsabile del procedimento valutare le modalità di spedizione (tradizionale o tramite posta elettronica) dei documenti.

Articolo 12 - Modalità di produzione e autenticazione dei documenti

I documenti in partenza o interni prodotti dal Comune di Gatteo, indipendentemente dal supporto sul quale sono stati scritti, devono riportare, nella opportuna forma grafica e se disponibili, le seguenti informazioni:

- Stemma del Comune di Gatteo con dicitura "Comune di Gatteo";
- Settore ed eventuale Servizio ;
- Indirizzo del Comune: Piazza A. Vesi n° 6, 47030 Gatteo;
- Numero di telefono: 0541 934001;
- Numero di fax: 0541 933344;
- Indirizzo istituzionale di posta elettronica: cogatteo@comune.Gatteo.fo.it
- Data completa (luogo, giorno, mese, anno) scritta per esteso (Es. : Gatteo, 2 dicembre 2003);
- Numero di protocollo;
- Numero di repertorio (es.Numero di ordinanza, di decreto sindacale ecc.nel formato "Ordinanza n. ");
- Indice di classificazione composto da categoria, classe, sottoclasse, fascicolo e eventuali altre suddivisioni quando introdotte;
- Numero di collegamento o riferimento ad un eventuale precedente (Es.:Riscontro a vostro prot. n. .);
- Oggetto del documento;
- Nome del file (riportato a sinistra in basso, in fondo al testo del documento).
- Numero degli allegati;
- Descrizione degli allegati;
- Sigla del responsabile del procedimento amministrativo con relativa firma autografa *o digitale;*

Articolo 13 - Documenti soggetti a trattamento specifico e a registrazione particolare

Esistono tipologie di documenti che, per disposizioni normative o regolamentari, sono soggetti a forme di trattamento e registrazione particolare:

- Deliberazioni del Consiglio Comunale;
- Deliberazioni della Giunta Comunale;
- Decreti sindacali;
- Ordinanze sindacali;
- Determinazioni dirigenziali;
- Ordinanze dirigenziali;
- Contratti;

Tali documenti possono non essere protocollati (art. 53, c. 5 DPR 445/2000). Ciascun complesso delle deliberazioni, dei decreti, delle determinazioni, delle ordinanze sindacali o dirigenziali, dei contratti costituisce una serie. La registrazione consiste nell'apposizione di un numero progressivo riferito alla serie di appartenenza, che per le deliberazioni, le determinazioni, i decreti e le ordinanze riparte da 1 ogni anno, mentre i contratti sono identificati con un numero di repertorio che prosegue di anno in anno. Per ogni deliberazione, decreto, ordinanza, determinazione devono essere redatti un originale ed una copia, dei quali il primo va conservato nella rispettiva serie e ordinato secondo il numero progressivo dell'anno, il secondo deve essere inserito nel rispettivo fascicolo, insieme agli altri documenti che afferiscono al medesimo procedimento amministrativo.

SEZIONE III - FUNZIONI, COMPETENZE, ATTIVITÀ DEL COMUNE: TITOLARIO DI CLASSICAZIONE

Nell'esercizio della propria autonomia - statutaria, normativa, organizzativa, amministrativa, impositiva e finanziaria - e nell'espletamento delle funzioni amministrative, proprie e delegate, relative alla popolazione e al territorio comunale, il Comune produce e riceve atti e documenti che, nel loro complesso, costituiscono l'archivio comunale.
Una opportuna gestione della documentazione è indispensabile per garantire il corretto svolgimento dell'attività amministrativa, e costituisce il presupposto per garantire i diritti di accesso ai documenti amministrativi e la possibilità di partecipare al procedimento riconosciuti dalla legge 241 del 7 agosto 1990.
Lo strumento per consentire la corretta e razionale organizzazione della documentazione è stato individuato, prima dalla dottrina archivistica e successivamente anche dalla normativa(art. 64, c. 4 del DPR 445/2000), nella classificazione dei documenti.

Articolo 14 - La classificazione dei documenti

La classificazione è un'attività di organizzazione logica di tutti i documenti correnti, ricevuti, spediti e interni, protocollati e non: essa stabilisce in quale ordine reciproco i documenti si organizzino nello svolgimento dell'attività amministrativa.
Per questo motivo "sono soggetti a classificazione tutti i documenti che entrano a far parte del sistema documentario" del Comune, a prescindere dal supporto utilizzato (cartaceo o informatico) e dallo stato di trasmissione (documenti ricevuti, spediti, interni). Lo scopo della classificazione è quello di individuare, all'interno di uno schema generale relativo al complesso delle competenze del Comune, l'ambito specifico all'interno del quale si colloca il documento (più precisamente, il procedimento, il fascicolo o la serie a cui appartiene il documento). L'attribuzione di un indice di classificazione, derivante da uno schema strutturato gerarchicamente, serve ad assegnare a ciascun documento un codice identificativo che, integrando (quando presente) il numero di protocollo, colleghi il documento in maniera univoca ad una determinata unità archivistica, generalmente un fascicolo.
Occorre sottolineare che lo schema di classificazione, per possedere una certa stabilità, fa riferimento alle competenze del Comune indipendentemente dai Settori e Servizi che concretamente le esercitano: mentre l'organizzazione dei Settori e dei servizi, infatti, può variare con relativa frequenza, le competenze dell'Ente rimangono sostanzialmente stabili nel tempo (l'impianto di base, infatti, è lo stesso da più di un secolo).Il titolario di classificazione attualmente utilizzato è strutturato in **15** categorie che vanno dall'amministrazione all'assistenza, alla polizia urbana, alle finanze e contabilità, ai lavori pubblici, alle attività produttive, allo stato civile; ciascuna categoria a sua volta è articolata in un numero variabile di classi, che, a seconda della materia, possono essere suddivise in più

sottoclassi. Eventuali modifiche possono essere concordate con il responsabile del Servizio Archivio ed adottate con apposito provvedimento. Il titolario attualmente utilizzato è riportato nell'allegato n. 1.

a) Allegato 1: Titolario di classificazione ed Indice

Articolo 15 - Uso del titolario: classificazione e fascicolazione dei documenti

Quando viene protocollato un documento che dà avvio ad una nuova pratica (ad un nuovo procedimento), ad esso deve essere attribuito un indice di classificazione composto dal riferimento alla categoria, alla classe nel cui ambito la pratica si colloca, seguiti dal numero del fascicolo. Ad esempio, il documento che dà avvio ad una pratica di assunzione avrà indice 1.8.3; in cui il primo 1 fa riferimento alla categoria 1. *Amministrazione*, l'8 alla classe ottava *Personale* della categoria 1, il 3 al fascicolo del *Personale*, cioè *Assunzioni*. Per il prossimo futuro è ipotizzabile l'introduzione di una numerazione cronologica e progressiva dei fascicoli allo scopo di meglio organizzare l'archiviazione della documentazione. Nell'esempio riportato dell'assunzione di personale, tutti i documenti relativi a quel procedimento di assunzione avranno numeri di protocollo diversi, ma lo stesso indice di classificazione 1.8.3/1, mentre gli atti relativi a procedimenti avviati successivamente nel corso dell'anno avranno di volta in volta, come indice, 1.8.3/2, 1.8.3/3 ecc.. Questo sistema di classificazione dovrebbe costituire la base a partire dalla quale i vari documenti ed atti prodotti e ricevuti dai singoli uffici dovrebbero essere organizzati fisicamente, oltre che logicamente.

Articolo 16 - Documenti appartenenti a fascicoli già esistenti

Quando il documento protocollato è relativo ad un procedimento o affare già in corso, il responsabile del procedimento a cui è stato assegnato il documento provvederà a inserirlo nel fascicolo di competenza, verificando che la classificazione sia corretta ed integrandola con la notazione relativa al fascicolo.

Articolo 17 - Il repertorio dei fascicoli

Il repertorio dei fascicoli è uno strumento che al momento non è ancora utilizzato correntemente presso gli uffici del Comune di Gatteo, ma la cui introduzione potrebbe agevolare sensibilmente la corretta gestione dei documenti e il loro rapido reperimento. Si è scelto di descriverne la struttura e le funzioni in modo che in questa prima fase ciascun Settore e Servizio possa decidere se adottarlo per la propria documentazione, in previsione di una futura estensione del suo uso a tutto l'Ente.
Per repertorio dei fascicoli si intende l'elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe , contenente, oltre all'oggetto dell'affare o del procedimento amministrativo, l'indice di classificazione completo (categoria, classe e numero del fascicolo). Sul repertorio dei fascicoli deve essere annotata anche la movimentazione dei fascicoli da un ufficio all'altro e dall'archivio corrente a quello di deposito. Il repertorio dei fascicoli ha cadenza annuale (inizia il 1 gennaio e termina il 31 dicembre di ciascun anno).

Articolo 18 – Organigramma del Comune

Le funzioni affidate o delegate al Comune e le attività ad esse connesse vengono attuate e poste in essere attraverso la struttura organizzativa propria dell'Ente. Con la deliberazione n. 88 del 19.06.1999 la Giunta Comunale ha definito la macrostruttura del Comune di Gatteo, indicando le linee fondamentali di organizzazione degli uffici e dei servizi comunali, mentre l'organizzazione interna ai

Settori è determinata dai singoli Responsabili. Dalla deliberazione n° 88 deriva l'attuale organigramma dell'Ente.

b) Allegato 3 – Organigramma del Comune di Gatteo

SEZIONE IV - DESCRIZIONE DEL SERVIZIO ARCHIVIO: ISTITUZIONE E FUNZIONI

Articolo 19 - L'Archivio del Comune di Gatteo

L'Archivio del Comune di Gatteo è costituito dal complesso dei documenti prodotti e acquisiti dall'Ente nello svolgimento della propria attività e nell'esercizio delle proprie funzioni. Esso comprende anche i fondi archivistici di enti e istituti cessati, le cui funzioni e/o proprietà sono state trasferite al Comune, e gli archivi e i documenti acquisiti per dono, deposito, acquisto o a qualsiasi altro titolo. L'Archivio è unico; le suddivisioni in archivio corrente, archivio di deposito e archivio storico sono solo gestionali. Indipendentemente dalla collocazione fisica del materiale che costituisce l'Archivio, e dal Settore che lo conserva, le modalità tecniche e operative per la gestione, tenuta, selezione e conservazione dei documenti appartenenti all'Archivio del Comune sono dettate dal responsabile del Servizio Archivio.

Articolo 20 - Il Servizio Archivio

Con la deliberazione della Giunta Comunale che approva il presente manuale viene istituito il Servizio per la tenuta del protocollo informatico, della gestione informatica del flussi documentali e degli archivi previsto dall'art. 61 del DPR 445/2000, individuandolo nel preesistente ufficio Protocollo e Archivio del Settore Affari Generali e Istituzionali. Tale Servizio, denominato per brevità Servizio Archivio, sovrintende alla gestione documentale dal protocollo all'archivio storico, a norma del citato art. 61, c.3:

- svolgendo i compiti di attribuzione del livello di autorizzazione per l'accesso alle funzioni della procedura,
- garantendo il rispetto delle disposizioni normative nelle operazioni di registrazione e segnatura di protocollo,
- garantendo la produzione e conservazione del registro giornaliero di protocollo,
- curando il ripristino delle funzionalità del sistema in caso di guasti,
- garantendo il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali,
- autorizzando le operazioni di annullamento,
- vigilando sull'osservanza delle disposizioni del testo unico sulla documentazione amministrativa,
- indicando le modalità tecniche ed operative per la gestione e la tenuta dei documenti,
- provvedendo ad elaborare un piano di conservazione e selezione e ad attivare le procedure necessarie ad una corretta selezione dei documenti,
- curando il riordinamento, la schedatura e l'inventariazione dei fondi archivistici, direttamente o tramite operatori qualificati,
- fornendo consulenza per la consultazione.

Il responsabile del Servizio Archivio si occupa inoltre della redazione e dell'aggiornamento del Manuale di Gestione.

SEZIONE V - IL SERVIZIO DI PROTOCOLLO

Articolo 21 - Unicità del protocollo

Il registro di protocollo del Comune di Gatteo è unico; esso è gestito dal Servizio Archivio ed è generato tramite apposita procedura informatica, che è utilizzabile da più stazioni contemporaneamente e che assegna automaticamente il numero (e la data) di protocollo a ciascun documento registrato. Come già dichiarato, all'unico registro di protocollo corrisponde un unico archivio, che può essere gestito con modalità differenziate e custodito in luoghi diversi, ma che rimane una unica entità. Ciascun Settore e Servizio, nel corso dello svolgimento della propria attività istituzionale, riceve, produce e invia atti e documenti appartenenti ai procedimenti amministrativi di cui il Settore o Servizio è responsabile. Tali atti e documenti fanno parte integrante a tutti gli effetti dell'archivio comunale, e vengono registrati tramite il protocollo generale. Considerando che la produzione dei documenti e l'attività amministrativa da cui i documenti scaturiscono sono poste in essere all'interno di ciascun Settore o Servizio, il Servizio Archivio delega ai singoli Settori e Servizi la facoltà di protocollare i documenti in partenza e di gestire e custodire i documenti dell'archivio corrente (e, in alcuni casi, dell'archivio di deposito). Dal 2003, con l'attivazione delle stazioni di protocollazione decentrate in tutti i Settori comunali, non sono né possono essere più utilizzati protocolli diversi dal protocollo generale. Sono tuttavia consentite forme di registrazione particolare per alcune tipologie di documenti (ad es.: denunce I.C.I., documenti relativi alla tenuta dei registri di stato civile ecc.). Il Servizio Archivio provvede alla ricezione e protocollazione di tutta la corrispondenza in arrivo, mentre quella in partenza è protocollata dall'ufficio che ciascun Settore o Servizio ha deputato a questo scopo. Il responsabile del Servizio Archivio provvede inoltre a definire le modalità per la gestione dei documenti, a raccogliere e coordinare eventuali esigenze di modifica dello schema di classificazione e della procedura.

Articolo 22 - Il Protocollo come atto pubblico

Tutti i documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi devono essere protocollati. Il registro di protocollo, infatti, da un punto di vista *giuridico* è un atto pubblico destinato a far fede della data di ricevimento o di spedizione dei documenti trattati da una pubblica amministrazione. Ciascun documento, prodotto o ricevuto da un'amministrazione e da questa protocollato, può essere univocamente identificato attraverso quattro elementi essenziali, più uno per i documenti informatici (file):

- il numero di protocollo (che deve essere unico per ciascun documento),
- la data di arrivo o di partenza,
- il mittente o destinatario
- l'oggetto
- l'impronta del documento, quando viene protocollato un documento informatico (da sperimentare).

Affinché possa esistere certezza sulla veridicità delle registrazioni, è necessario garantire che l'interrelazione tra questi elementi essenziali sia costante ed immodificabile.

Articolo 23 - Informazioni minime

La registrazione di protocollo per ogni documento ricevuto, spedito o interno, a norma dell'art. 53 DPR 445/2000, è effettuata mediante la memorizzazione delle seguenti informazioni:

a) Numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
b) Data di registrazione del protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

c) Mittente (o mittenti) per i documenti ricevuti, o, in alternativa, destinatario (o destinatari) per i documenti spediti, registrati in forma non modificabile;
d) Oggetto del documento, registrato in forma non modificabile;
e) Data e protocollo del documento ricevuto, se disponibili;
f) Impronta del documento informatico, se trasmesso per via telematica, generata impiegando la funzione di hash SHA-1 e registrata in forma non modificabile.

Articolo 24 - Oggetto riservato

Qualora l'oggetto del documento contenga dati sensibili, l'operatore deve adottare le misure atte a garantire la riservatezza dei dati stessi, utilizzando le funzionalità presenti nella procedura del protocollo informatico e descritte nel Manuale operativo.

Articolo 25 - Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo del documento stesso: l'indicazione "Comune di Gatteo", il numero e la data di protocollo, l'eventuale indicazione del Settore o Servizio, il codice di classificazione (cfr. art. 55 DPR 445/2000). La registrazione e la segnatura di protocollo costituiscono un'operazione unica e contestuale. Il codice di classificazione è assegnato in fase di protocollazione e può essere successivamente integrato dal responsabile del procedimento. Qualora debba essere modificato, la modifica deve essere concordata con il Servizio Archivio. Nel documento cartaceo in arrivo la segnatura viene posta di norma in calce al documento tramite un timbro recante la dicitura "Comune di Gatteo. Prot. N°…. ", data, "Protocollo Generale". L'indicazione del numero di protocollo è immediatamente successiva all'attribuzione alla registrazione del numero di protocollo da parte della procedura informatica. Per i documenti in partenza o interni, la segnatura può essere apposta tramite timbro, o indicata nel testo del documento

Articolo 26 - Annullamento di una registrazione o dei dati di una registrazione

E' consentito l'annullamento delle registrazioni di protocollo o dei dati di una registrazione di protocollo. In particolare l'annullamento delle informazioni generate o assegnate automaticamente dal sistema in forma non modificabile (data, ora e numero di protocollo), comporta l'automatico e contestuale annullamento della intera registrazione di protocollo. Le registrazioni annullate rimangono memorizzate e visibili, e deve essere possibile visualizzare la data di annullamento, l'operatore che lo ha effettuato e gli estremi del provvedimento di autorizzazione. Delle altre informazioni, registrate in forma non modificabile (mittente o destinatario, oggetto), l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione dati, è consentito con gli stessi criteri che valgono per le registrazioni annullate: esse rimangono memorizzate e visibili, e deve essere possibile visualizzare la data ed ora di annullamento, l'operatore che lo ha effettuato e gli estremi del provvedimento di autorizzazione. Solo il responsabile del Servizio Archivio è autorizzato ad annullare le registrazioni o i dati delle registrazioni. E' istituito un apposito registro per le autorizzazioni delle operazioni di annullamento delle registrazioni e delle informazioni di protocollo. Tutte le altre informazioni relative ad una registrazione di protocollo sono modificabili dall'autore o da chi ha in carico il procedimento.

Articolo 27 - Documenti da non protocollare

L'elenco delle tipologie di documenti che possono essere non protocollati è contenuto nell'allegato 4.

Allegato 4 – Documenti da non protocollare

Articolo 28 - Registro di emergenza

Ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema di protocollo informatico, il responsabile della tenuta del protocollo informatico, autorizza la protocollazione manuale dei documenti su un registro di emergenza. La protocollazione manuale di emergenza deve essere effettuata in maniera accentrata, esclusivamente presso il servizio protocollo. Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico previste dall'art. 63 del T.U. e precisamente:

- Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora di ripristino della funzionalità del sistema.
- Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile del servizio può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione.
- Per ogni giornata di registrazione di emergenza è riportato sul registro il numero totale di operazioni registrate.
- La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l' identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.
- Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

Articolo 29 - Il registro di protocollo

Il registro di protocollo è un atto pubblico 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 a favore o a danno delle parti. Il registro di protocollo è di norma un documento informatico. Il responsabile del Servizio Archivio provvede quotidianamente alla stampa del registro giornaliero di protocollo. Entro il mese di gennaio il responsabile del Servizio Archivio provvede altresì alla stampa integrale (aggiornata con i rinvii reciproci ai numeri precedenti e successivi) del registro di protocollo dell'anno precedente e, verificata la congruità delle registrazioni, allo scarto dei singoli fogli accumulati quotidianamente delle stampe del registro giornaliero dell'anno precedente. Quando il repertorio dei fascicoli sarà utilizzato correntemente, il responsabile del Servizio Archivio provvederà a stamparlo contestualmente al registro di protocollo annuale.

SEZIONE VI - DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Articolo 30 Documenti in arrivo

La protocollazione e lo smistamento della corrispondenza in arrivo spettano unicamente al Servizio Archivio, a cui deve essere convogliata tutta la documentazione comunque pervenuta al Comune dall'esterno, tramite consegna manuale, servizio postale, corriere, fax, posta elettronica o eventuali altri sistemi. Per questo motivo è necessario, nei rapporti con l'esterno, indicare costantemente come indirizzo "**Comune di Gatteo Piazza A.Vesi 6 – 47030 Gatteo**", come fax il n. **0541/933344,** e come indirizzo istituzionale di posta elettronica il seguente: **"cogatteo@comune.gatteo.fo.it."**. Nei casi in cui la documentazione pervenga o sia consegnata ad uffici diversi dal Protocollo generale, è necessario che venga comunque tempestivamente inoltrata al Servizio Archivio per la necessaria

protocollazione, eventualmente utilizzando il fax per i casi più urgenti. L'indicazione dell'indirizzo nel caso di pacchi e merci deve invece riportare con chiarezza l'ufficio destinatario.

Articolo 31- Rilascio di ricevuta di un documento consegnato a mano

A richiesta dell'interessato, l'Ufficio Protocollo appone un timbro datario su una fotocopia del documento consegnato a mano all'Ufficio stesso. Tale fotocopia ha valore di ricevuta. Dal giorno lavorativo successivo a quello della consegna è possibile rivolgersi all'Ufficio Protocollo per conoscere il numero di protocollo che è stato assegnato al documento.

Articolo 32- Apertura della corrispondenza

Al fine di evitare movimentazioni inutili, dal momento che pressoché la totalità della corrispondenza che giunge al Comune tramite il servizio postale riguarda l'attività amministrativa dell'Ente, anche quando è indirizzata nominativamente, si è stabilito di aprire tutta la corrispondenza sulla quale non sia riportata una dicitura del tipo "Riservata", "Personale", "Confidenziale" ecc.

Articolo 33 - Lettere anonime

Dal momento che una delle funzioni più importanti del registro di protocollo è essenzialmente quella di attestare che un determinato documento è pervenuto presso l'Ente o è partito da un suo Settore / Servizio, le lettere anonime vengono protocollate per testimoniarne l'arrivo, indicando "Anonimo" nel campo del mittente, contrassegnando l'oggetto come "Riservato" e utilizzando per identificarle il codice aggiuntivo ANON.

Articolo 34 - Data di protocollazione

La protocollazione avviene di norma entro il giorno lavorativo successivo a quello in cui gli atti e documenti pervengono al Protocollo generale. Casi di particolare urgenza possono sempre essere segnalati al Protocollo generale, che in ogni caso si adopera per soddisfare le esigenze degli altri Settori / Uffici.

Articolo 35 - Protocollazione di offerte

Non vengono aperti, e sono protocollati chiusi, plichi e buste che riportano indicazioni del tipo "Offerta" o "Gara", o dalla cui confezione si possa evincere la partecipazione ad una gara: al momento dell'apertura, il numero di protocollo apposto sulla busta va poi riportato, a cura del responsabile del procedimento, sui documenti contenuti nella busta, mantenendo comunque la busta come allegato. Per evitare ritardi e garantire una più efficiente gestione delle procedure relative allo svolgimento delle gare, i vari Settori provvedono a comunicare all'Ufficio Protocollo l'indizione e la scadenza di gare ed offerte. Quando possibile, specie nei casi di gare o in quelli in cui è prevedibile l'arrivo di una considerevole mole di documenti, si evita di fissare la scadenza per la consegna nella giornata di sabato.

Articolo 36 - Messaggi telefax

L'uso del telefax soddisfa il requisito della forma scritta e quindi il documento pervenuto via fax può **non** essere seguito da altro originale. Dal momento che ogni documento deve essere individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, qualora venga registrato un documento via telefax e venga successivamente ricevuto lo stesso documento in originale, è necessario attribuire all'originale la stessa segnatura di protocollo del documento pervenuto via telefax (si tratta del medesimo documento su diverso supporto e con diverso mezzo di

trasmissione). Qualora si rilevi che l'originale è stato registrato con un diverso numero di protocollo, la registrazione relativa all'originale deve essere annullata. Se tuttavia tra il documento pervenuto via fax e l'originale ricevuto con altro mezzo vi sono differenze anche minime, si debbono considerare documenti diversi e quindi l'originale dovrà essere registrato con un nuovo numero di protocollo. Il timbro di protocollo va apposto di norma sul documento e non sulla copertina di trasmissione del telefax.

Articolo 37 - Posta elettronica

Il Comune di Gatteo ha definito una casella di posta elettronica, denominata casella istituzionale, **adibita a finalità di ricezione dei documenti informatici,** che al momento vengono trasformati in documenti analogici per la protocollazione. Il suo indirizzo è: cogatteo@comune.gatteo.fo.it .Questo indirizzo di posta elettronica viene pubblicizzato sul sito web comunale, insieme con le modalità di inoltro della corrispondenza ed i tipi di documenti che possono essere inviati all'ente. L'addetto dell'ufficio preposto allo smistamento delle e-mail controlla i messaggi pervenuti nella casella di posta istituzionale e verifica se siano o meno da protocollare. Se non sono da protocollare li inoltra direttamente al Settore o Servizio competente; se invece sono da protocollare, li inoltra al Protocollo Generale che li stampa, li protocolla e appone sulla versione cartacea del documento la segnatura di protocollo. Successivamente l'addetto al protocollo inoltra via posta elettronica i messaggi al Responsabile del Servizio, specificando il numero di protocollo assegnato al documento, mentre la versione cartacea con la segnatura di protocollo viene smistata come qualsiasi altro documento cartaceo. Verranno protocollati solamente i messaggi inviati alla casella istituzionale di posta elettronica. I messaggi eventualmente pervenuti ad una casella diversa da quella istituzionale dovranno essere reindirizzati dai destinatari alla casella di posta istituzionale.

Articolo 38 - Smistamento

L'Ufficio protocollo smista la corrispondenza in arrivo, aperta e protocollata, indirizzando l'originale di ciascun documento al Settore che, per quanto a conoscenza dell'Ufficio protocollo stesso, ha competenza sull'oggetto specificato nel documento: così come il documento, anche la registrazione di protocollo sulla procedura informatica risulta "in carico" ad un determinato servizio, che è l'unico, insieme al Protocollo generale, che può apportarvi modifiche ed integrazioni. Ad altri Servizi o organi comunali, indicati sull'originale successivamente al primo, può essere inviata una copia del documento per conoscenza. Quotidianamente ciascun servizio provvede al ritiro della posta assegnata.

Articolo 39 - Assegnazione

Il Responsabile del Servizio, o un suo incaricato ,provvede ad assegnare ciascun documento in arrivo al responsabile del relativo procedimento amministrativo. Spettano al responsabile del procedimento amministrativo le incombenze relative alla gestione del documento: l'inserimento nel fascicolo di competenza preesistente o eventualmente in un nuovo fascicolo, l'integrazione o la correzione del codice di classificazione assegnato dal Protocollo generale, l'effettuazione, tramite la procedura del protocollo informatico, dei collegamenti ai protocolli precedenti.

Articolo 40 - Variazioni nel Settore di carico di un documento

Nel caso in cui un Settore riceva un documento originale relativo a materie estranee alla propria specifica competenza, oppure, a causa di un disguido o di un errore, un documento indirizzato ad altri, il Responsabile può scegliere:

a) **Di far recapitare all'Ufficio protocollo il documento per l'invio al Settore competente**; l'Ufficio protocollo provvederà anche a registrare l'avvenuta movimentazione sul registro di protocollo, oppure
b) **Di inoltrare direttamente il documento al Settore competente**, curando che tale passaggio di competenze venga registrato sul protocollo tramite la funzionalità "note".

Articolo 41 - Passaggio per competenza da un Ufficio ad un altro per acquisizione pareri ecc.

Quando, nel corso dell'iter di un procedimento, un documento debba passare da un servizio ad un altro per l'acquisizione di pareri ecc., **il servizio che ha in carico il documento e che lo trasmette ad altra unità organizzativa deve provvedere a segnalare il passaggio anche sul protocollo**, tramite la funzionalità "Richiesta pareri", in modo che sia sempre possibile sapere dove si trova il documento e chi ne ha la responsabilità.

Articolo 42 - Documento inviato in copia ad altri uffici

Qualora il responsabile del procedimento ritenga opportuno portare altri uffici a conoscenza del contenuto di un documento inviandogliene una copia, deve provvedere altresì ad aggiungere tale informazione sul protocollo informatico.

Articolo 43 - Documenti interni

Tutti i documenti interni rilevanti dal punto di vista giuridico -probatorio devono essere protocollati in partenza dai singoli servizi ed inviati ai destinatari utilizzando il servizio di posta elettronica.

Articolo 44 - Documenti in partenza

I documenti posti in essere da personale in servizio presso il Comune nello svolgimento delle proprie funzioni e destinati all'esterno dell'Ente sono protocollati, a cura del responsabile del procedimento, di norma da una delle stazioni di protocollazione situate nel Settore di appartenenza. In fase di protocollazione devono essere attuati i collegamenti ai documenti registrati precedentemente appartenenti allo stesso fascicolo. La trasmissione dei documenti all'esterno dell'Ente può avvenire per mezzo del servizio postale (lettera semplice, raccomandata, posta prioritaria, posta celere ecc.), per mezzo di corrieri o via telefax per i documenti analogici, e tramite posta elettronica per i documenti informatici. La scelta del mezzo di trasmissione più opportuno, quando non espressamente indicata dalla normativa vigente, spetta al responsabile del procedimento amministrativo. Nel caso di trasmissione via telefax, non si spedisce l'originale per mezzo del servizio postale se non su espressa richiesta del destinatario. Sull'originale del documento inserito nel fascicolo del procedimento dovrà essere posta la dicitura "Trasmesso via telefax"; la copertina del fax e il rapporto di trasmissione dovranno essere anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione. Per trasmettere un documento via posta elettronica il responsabile del procedimento dopo averlo redatto lo protocolla e produce contestualmente anche un originale cartaceo,dotato degli elementi di cui all'art.12, da inserire ne fascicolo del procedimento.

SEZIONE VII - GESTIONE E CONSERVAZIONE DEI DOCUMENTI

Articolo 45 - Archivio corrente

Per archivio corrente si intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi non ancora conclusi. Tale documentazione è custodita direttamente dal responsabile del procedimento, che è responsabile anche della corretta organizzazione e gestione e della classificazione dei documenti che tratta, indipendentemente dal supporto e dalle modalità di trasmissione.

Articolo 46 - Fascicoli e Serie

I documenti possono essere aggregati sulla base dell'affare o del procedimento cui si riferiscono, oppure sulla base della loro omogeneità di forma (delibere, contratti, mandati di pagamento ecc.). Nel primo caso si formano dei fascicoli, nel secondo delle serie. La scelta di organizzare i documenti in un modo piuttosto che in un altro dipende esclusivamente da esigenze funzionali, e, per determinate tipologie di documenti (delibere, determine ecc.) è opportuno che dello stesso documento vengano redatti un originale e, almeno, una copia che va inserita nel fascicolo di competenza, mentre l'originale va conservato nella serie relativa. A ciascun fascicolo e a ciascuna serie è attribuito un indice di classificazione specifico, capace, insieme alla data di istruzione e all'oggetto, di identificarli univocamente.

Articolo 47- Chiusura di un fascicolo

Quando il procedimento amministrativo o l'affare è concluso, il relativo fascicolo deve essere chiuso prima di passare all'archivio di deposito. Le operazioni di chiusura del fascicolo comprendono la verifica dell'ordinamento e l'identificazione delle copie, fotocopie ecc. che possono essere eliminate nell'ambito delle attività di selezione e scarto.

Articolo 48 - Archivio di deposito

Per archivio di deposito si intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi da meno di 40 anni, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico.

Articolo 49 - Selezione e scarto

Nell'ambito dell'archivio di deposito vengono effettuate le operazioni di selezione e scarto, curate dal Servizio Archivio in collaborazione con il Settore che conserva la documentazione. La selezione viene effettuata attualmente sulla base dei massimari di scarto per gli archivi comunali. In futuro, laddove adottato, potrà essere effettuato sulla base di uno specifico piano di conservazione del Comune di Gatteo. I documenti selezionati per l'eliminazione devono essere descritti in un elenco contenente i riferimenti alle categorie del titolario di classificazione, il numero e la tipologia delle unità archivistiche (faldoni, fascicoli, registri ecc.), gli estremi cronologici, la descrizione della documentazione e un'indicazione sommaria del peso. Tale elenco, sotto forma di proposta di scarto, deve essere trasmesso alla Soprintendenza Archivistica per la concessione della necessaria autorizzazione. Ottenuta l'autorizzazione, la Giunta delibera lo scarto dei documenti contenuti nell'elenco. Successivamente alla deliberazione della Giunta è possibile conferire il materiale per la distruzione. Le operazioni di selezione e scarto sono sempre preliminari al passaggio della documentazione all'archivio storico, o comunque alla consegna al Servizio Archivio.

Articolo 50 - Archivio storico

Per archivio storico si intende il complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa effettuazione delle operazioni di scarto, alla conservazione permanente per finalità storiche e culturali. Il Comune provvede al riordinamento del proprio patrimonio documentario e all'inventariazione dell'archivio storico, e a consentire la consultazione per finalità storiche e scientifiche.

Articolo 51 - Riproduzione di documenti

I documenti appartenenti all'archivio di deposito e all'archivio storico possono essere fotocopiati solamente se da tale operazione non derivi danno al documento stesso. I documenti che non possono essere fotocopiati per ragioni di conservazione possono sempre essere fotografati. La fotocopiatura o l'eventuale fotografia dei documenti devono svolgersi all'interno dei locali comunali. Per particolari documentate esigenze, il responsabile del Servizio Archivio può autorizzare lo svolgimento di tali operazioni al di fuori dei locali comunali.

SEZIONE VIII - DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

Articolo 52 - Descrizione funzionale

La descrizione funzionale del protocollo informatico è costituita dal Manuale Utente fornito dalla ditta produttrice del sistema, aggiornato alla release in uso, disponibile on line e consultabile da ogni operatore addetto alla protocollazione attraverso una specifica funzione del programma.

SEZIONE IX - MODALITÀ DI PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Articolo 53 - Registrazione di protocollo

Ogni registrazione di protocollo è generata nel momento in cui l'operatore, avendo inserito i dati relativi al documento che sta protocollando, conferma l'inserimento: il sistema genera un nuovo numero di protocollo ed attribuisce automaticamente la data e l'ora di protocollazione. La procedura del protocollo informatico non è attualmente collegata automaticamente ad un sistema di segnatura: in attesa di disporre di soluzioni tecnologiche adeguate, si è scelto di utilizzare dei timbri datari con dicitura "Comune di Gatteo – Protocollo generale" da apporre sulla prima pagina dei documenti: non appena la procedura assegna il numero di protocollo, questo viene riportato manualmente sul timbro precedentemente apposto. Per i documenti in partenza o interni prodotti con strumenti informatici, il numero di protocollo può essere inserito direttamente nel testo del documento prima dell'eventuale stampa.

SEZIONE X - ACCESSIBILITA' AL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Articolo 54 Accessibilità da parte degli utenti appartenenti all'area organizzativa omogenea

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password, od altre tecniche e dispositivi di autenticazione sicura.
L'operatore che effettua la registrazione di protocollo inserisce il livello di riservatezza richiesto per il documento in esame, se diverso da quello standard applicato automaticamente dal sistema.
In modo analogo, l'ufficio che effettua l'operazione di apertura di un nuovo fascicolo ne determina anche il livello di riservatezza.
Il livello di riservatezza applicato ad un fascicolo è ereditato automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. Quelli che invece hanno un livello di riservatezza superiore lo mantengono.
Per quanto concerne i documenti sottratti all'accesso, si rinvia allo specifico Regolamento per la disciplina del procedimento amministrativo e dell'accesso agli atti e ai documenti amministrativi.
I livelli di riservatezza gestiti dal sistema, il livello standard applicato automaticamente e le relative abilitazioni all'accesso interno alle informazioni documentali sono riportati nell'allegato.

Articolo 55 - Accesso esterno

L'accesso al sistema di gestione informatica dei documenti da parte di utenti esterni sarà realizzato mediante l'impiego di sistemi di riconoscimento ed autenticazione sicura basati sulla carta d'identità elettronica e sulla firma digitale.
Sono rese disponibili tutte le informazioni necessarie e sufficienti all'esercizio del diritto di accesso ai documenti amministrativi.

Articolo 56 Accesso da parte di altre pubbliche amministrazioni

L'accesso al sistema di gestione informatica dei documenti da parte di altre pubbliche amministrazioni, è realizzato applicando le norme ed i criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni.

ALLEGATI

Allegato 1 :Titolario di Classificazione

Allegato 2: Organigramma del Comune

Allegato 3: Documenti da non protocollare

Allegato 4: Funzionalità del Sistema di gestione documentale e conformità normativa AIPA

Allegato 5: Piano della Sicurezza Informatica

Allegato 6: Abilitazione all'utilizzo del Sistema di gestione informatica dei documenti, livelli di riservatezza e corrispondenti logiche di protezione

Allegato 7: Presentazione del Progetto Panta Rei

Allegato 1 - Titolario d’archivio

Allegato 2 – Organigramma del Comune

ALLEGATO N° 3

DOCUMENTI CHE POSSONO ESSERE ESCLUSI DALLA PROTOCOLLAZIONE

⇒ DOCUMENTI CHE POSSONO NON ESSERE PROTOCOLLATI

Le seguenti tipologie di documenti possono non essere protocollate:

1. **Pubblicazioni:**
   - ✓ Gazzette ufficiali
   - ✓ Bollettino ufficiale della Regione Emilia-Romagna
   - ✓ Notiziari di Amministrazioni pubbliche
   - ✓ Giornali
   - ✓ Riviste
   - ✓ Libri
2. **Materiali statistici**
3. **Atti preparatori interni**
4. **Materiali pubblicitari**
5. **Inviti a manifestazioni che non attivino procedimenti amministrativi**
6. **Certificati anagrafici rilasciati direttamente al richiedente**
7. **Documenti di occasione, di interesse effimero, quali:**
   - ✓ Ringraziamenti
   - ✓ Richieste di appuntamenti con il Sindaco
   - ✓ Congratulazioni varie
   - ✓ Condoglianze

⇒ DOCUMENTI SOGGETTI – DIRETTAMENTE O INDIRETTAMENTE - A REGISTRAZIONE PARTICOLARE DEL COMUNE:

Le seguenti tipologie di documenti sono soggette a registrazione particolare:

- ✓ Deliberazioni del Consiglio Comunale
- ✓ Deliberazioni della Giunta Comunale
- ✓ Decreti del Sindaco
- ✓ Ordinanze sindacali
- ✓ Ordinanze dirigenziali
- ✓ Determinazioni dirigenziali
- ✓ Convocazioni di Commissioni consiliari
- ✓ Mod. APR/4
- ✓ Documentazione relativa alla istruzione e formazione dell'elenco preparatorio della leva militare
- ✓ Documenti per la gestione ruoli matricolari

- ✓ Documenti per la gestione elenco preparatorio lista di leva (corrispondenza tra comuni)
- ✓ Assicurazione di avvenuta trascrizione atto di nascita
- ✓ Richiesta copia integrale dell'atto di nascita da parte di altri comuni per procedere alla pubblicazione di matrimonio
- ✓ Comunicazione da parte di altri comuni dell'eseguita trascrizione dall'atto di morte nei registri di stato civile con gli estremi
- ✓ Dichiarazioni I.C.I.
- ✓ Certificazione di applicazione dei parametri di cui all'accordo territoriale
- ✓ Verbali di infrazione al Codice della Strada
- ✓ Verbali di violazioni amministrative ex L. n°689/1981
- ✓ Permessi di costruzione

Allegato 4

Dichiarazione di conformità dell'applicativo Progetto Ente – Protocollo e Atti

L'AIPA, centro tecnico del ministero per l'innovazione e le tecnologie, ha definito uno strumento per verificare la conformità di un sistema di protocollo informatico ai requisiti desumibili dal quadro normativo di riferimento. Questo strumento prende la forma di una Check List.

La Check List si rivolge:

- alle Amministrazioni Pubbliche, come supporto nella fase di acquisizione e nelle operazioni di collaudo di uno specifico sistema di protocollo informatico;
- alle Aziende produttrici di software, come strumento di test e verifica di conformità alla normativa delle funzionalità implementate.

La Check List prevede diversi livelli di conformità, in base agli obiettivi prefissati.
I livelli di "requisito" sono i seguenti:

- Requisito di livello **"A"**: rappresenta i requisiti richiesti per un sistema di protocollo informatizzato in modalità base, a volte citato come "nucleo minimo del protocollo".
- Requisito di livello **"AA"**: rappresenta i requisiti richiesti per la realizzazione di un sistema che rientra in uno scenario di "gestione informatica dei documenti e dei flussi documentali".
- Requisito di livello **"AAA"**: rappresenta le ulteriori funzionalità richieste in scenari che approfondiscono aspetti legati all'automazione dei flussi procedurali.
- La lettera **"B",** infine, individua i requisiti richiesti per l'interoperabilità.

Inoltre, è indicata la normativa che prevede lo specifico requisito; es: TU4452000/52/1/a, DPCM311000/7/1, AIPACIRC28/5.

L'applicativo *ProgettoEnte - Protocollo e Atti* risponde positivamente ai punti previsti dalla Check List come riportato nello schema allegato.

CHECK LIST

Tabella di Controllo – sezione 1

Requisito	S/N
A R.1.1 [TU4452000/52/1/a] Garanzie di sicurezza e integrità del sistema	**SI**
A R.1.2 [DPCM311000/7/1] Requisiti minimi di sicurezza del sistema operativo dell'elaboratore	**SI**
A R.1.3 [DPCM311000/7/2] Disponibilità di meccanismi che consentano il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti in condizioni di sicurezza nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali	**SI**
A R.1.4 [DPCM311000/7/3] Tracciamento da parte del sistema di protocollo informatico di qualsiasi evento di modifica delle informazioni trattate e individuazione del suo autore	**SI**
A R.1.5 [DPCM311000/7/4] Protezione delle registrazioni di tracciamento da modifiche non autorizzate	**SI**
A R.1.6 [TU4452000/52/1/b] Garanzie sulla corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita	**SI**
A R.1.7 [TU4452000/53/1/a] Generazione automatica del numero di protocollo e sua registrazione in forma non modificabile	**SI**
A R.1.8 [TU4452000/57/1] Il numero di protocollo è un numero progressivo e costituito da almeno sette cifre numeriche e la numerazione di protocollo è rinnovata ogni anno solare	**SI**
A R.1.9 [TU4452000/53/1/b] Generazione automatica della data di registrazione di protocollo e sua registrazione in forma non modificabile	**SI**
A R.1.10 [TU4452000/53/1/c] Registrazione in forma non modificabile del mittente per i documenti ricevuti o, in alternativa, del destinatario o dei destinatari per i documenti spediti	**SI**
A R.1.11 [TU4452000/53/1/d] Registrazione in forma non modificabile dell'oggetto del documento	**SI**
A R.1.12 [TU4452000/53/1/e] Possibilità di registrare la data e protocollo del documento ricevuto, se disponibili	**SI**
A R.1.13 [TU4452000/53/1/f] Registrazione in forma non modificabile dell'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto	**SI**
A R.1.14 [DPCM311000/17/2] L'impronta è generata utilizzando la funzione di hash, definita nella norma ISO/IEC 10118-3:1998, Dedicated Hash-Function 3, corrispondente alla funzione SHA-1	**SI**
A R.1.15 [TU4452000/53/3] Assegnazione delle informazioni nelle operazioni di registrazione di protocollo effettuata dal sistema in un'unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati	**SI**
A R.1.16 [TU4452000/54/1] [DPCM311000/8] Esistenza di una funzione di annullamento delle informazioni non modificabili delle registrazioni e/o dell'intera registrazione	**SI**
A R.1.17 [TU4452000/54/1] [DPCM311000/8] Memorizzazione delle informazioni annullate nella base di dati	**SI**
A R.1.18 [TU4452000/54/2] Mantenimento per le informazioni annullate di una dicitura o un segno in posizione sempre visibile e tale da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione	**SI**
A R.1.19 [TU4452000/55/1] Apposizione in forma permanente e non modificabile della segnatura di protocollo all'originale del documento	**SI**
A R.1.20 [TU4452000/55/1] [DPCM311000/9/1] Presenza nella segnatura di protocollo delle informazioni minime per l'identificazione univoca di ciascun documento: codice identificativo dell'Amministrazione, codice identificativo dell'Area Organizzativa Omogenea, progressivo di protocollo, data di protocollo	**SI**
A R.1.21 [TU4452000/55/2] L'operazione di segnatura del protocollo effettuata contemporaneamente all'operazione di registrazione di protocollo	**SI**
A R.1.22 [TU4452000/55/3] La segnatura di protocollo può includere ulteriori informazioni quali il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo	**SI**
A R.1.23 [TU4452000/53/2] Produzione del registro giornaliero di protocollo	**SI**

A R.1.24 [TU4452000/63/5] Esistenza di un'apposita funzione di recupero dei dati che consenta l'inserimento delle informazioni relative ai documenti protocollati in emergenza, in seguito ad interruzione nella disponibilità della procedura informatica, senza ritardo al ripristino delle funzionalità del sistema	**SI**
A R.1.25 [TU4452000/63/5] Attribuzione durante la fase di ripristino a ciascun documento registrato in emergenza di un numero di protocollo del sistema informatico ordinario	**SI**
A R.1.26 [TU4452000/63/5] Correlazione stabile tra il numero di protocollo del sistema informatico ordinario con il numero utilizzato in emergenza	**SI**
A R.1.27 [TU4452000/52/1/c] Fornitura da parte del sistema delle informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa, formati nell'adozione dei provvedimenti finali	**SI**
A R.1.28 [TU4452000/52/1/f] Disponibilità di funzioni per il supporto e la gestione del sistema di classificazione d'archivio (titolario d'archivio)	**SI**
A R.1.29 [*derivato*] Funzioni che consentano l'utilizzo di strumenti di navigazione grafica e di browsing all'interno del sistema di classificazione adottato (a fini di selezione, ricerca, visualizzazione)	**SI**
A R.1.30 [TU4452000/52/1/f] Corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato	**SI**
A R.1.31 [*derivato*] Funzione di numerazione progressiva automatica dei fascicoli	**SI**
A R.1.32 [*derivato*] Funzioni di gestione dei fascicoli	**SI**
A R.1.33 [*derivato*] Funzioni per la creazione, la gestione e la manutenzione dell'organigramma dell'amministrazione	**SI**
A R.1.34 [*derivato*] Il sistema deve gestire un indice dei corrispondenti in modo da facilitare le operazioni di protocollazione dei documenti ricevuti e spediti. Deve essere possibile effettuare delle ricerche ed alimentare l'indice attraverso le operazioni di protocollazione	**SI**
A R.1.35 [TU4452000/52/1/d] Reperimento delle informazioni riguardanti i documenti registrati	**SI**
A R.1.36 [TU4452000/58/2] Esistenza di criteri di selezione basati su tutti i tipi di informazioni registrate per la ricerca delle informazioni del sistema	**SI**
A R.1.37 [TU4452000/58/3] Possibilità di elaborazioni statistiche sulle informazioni registrate	**SI**

Tabella di Controllo Interoperabilità

B R.4.1 [DPCM311000/15/1] [TU4452000/14/1] Lo scambio dei documenti informatici soggetti alla registrazione di protocollo è effettuato mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni	**SI**
B R.4.2 [DPCM311000/15/2] Corrispondenza di un'unica operazione di registrazione di protocollo ad ogni messaggio di posta elettronica ricevuto da un'area organizzativa omogenea	**SI**
B R.4.3 [DPCM311000/18/1] I dati relativi alla segnatura di protocollo di un documento trasmesso da un'area organizzativa omogenea sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML) 1.0 (raccomandazione W3C 10 febbraio 1998), conforme con un file DTD (Document Type Definition) di cui alla circolare Aipa n. 28 del 7/5/2001, ovvero alla sua versione più recente	**SI**
B R.4.4 [DPCM311000/19/1] [DPCM311000/19/2] Requisito di completezza della segnatura informatica	**SI**

ALLEGATO 5

PIANO DELLA SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI AI SENSI DELL'ART. 4 COMMA C. DEL D.P.C.M. 31.10.2000 e del D.LGSL. 196/2003

Indice

Introduzione

Considerato la molteplicità dei trattamenti dei dati personali, anche sensibili, nell'ambito dell'Amministrazione Comunale, nonché la complessità del sistema degli archivi e delle banche dati informatizzate;

Ritenuto che a fronte delle finalità delle misure di sicurezza esposte all'articolo 5, comma 2, lett. b), del D.P.C.M. 31 ottobre 2000 e Decreto Legislativo 196/2003 , risulti opportuno riportare in un unico documento programmatico a contenuto organizzativo-operativo gli elementi di riferimento necessari per la formazione, gestione, interscambio, accesso e conservazione dei documenti informatici, avendo particolare riguardo per il trattamento delle banche dati contenenti dati personali e dati sensibili.

Dato atto che tali misure di sicurezza, periodicamente riviste e comunque soggette a reimpostazione annuale, costituiscono il riferimento per la definizione mediante apposite determinazioni dirigenziali, di soluzioni operative dettagliate, correlate alla specificità e alla complessità dei singoli settori;

Rilevato che l'assetto del quadro di misure riportato nel documento programmatico di seguito indicato è definito con riguardo a:
1. stato dell'informatizzazione del comune
2. gestione dei flussi documentali attraverso un sistema informatizzato di protocollazione generale;

Il presente Piano di sicurezza è stato redatto per definire le politiche di sicurezza informatica del sistema informatico comunale in materia di trattamento dei dati ed i criteri organizzativi per la loro attuazione in base alla normativa vigente in materia. Le attività che discendono dall'applicazione di tali norme sono le seguenti:

- **analisi dei rischi in relazione alla tipologia dei documenti;**
- **analisi dei rischi in relazione alla tipologia dei dati personali (D.lgs. 196/2003);**
- **misure di sicurezza da adottare di tipo organizzativo, procedurale e tecnico;**
- **formazione dei dipendenti;**
- **monitoraggio periodico del piano di sicurezza.**

Per essere efficaci le misure di sicurezza di un sistema informativo devono garantire il raggiungimento dei seguenti obiettivi:

1. **Riservatezza: ossia prevenzione dell'utilizzo indebito di informazioni riservate.**
2. **Integrità: ossia prevenzione delle alterazioni o manipolazioni indebite delle informazioni.**
3. **Disponibilità: ossia garanzia dell'accesso controllato alle informazioni**
4. **Verificabilità e controllabilità delle modalità di trattamento dei dati e delle operazioni svolte.**

Di questi obiettivi si è tenuto conto nel momento di progettazione del sistema informativo per connotarne l'architettura allo scopo di costituire un sistema informatico "sicuro" in relazione allo stato della tecnica in materia.

1. ADEMPIMENTI PRELIMINARI ALL'ADOZIONE DI MISURE DI SICUREZZA

Il raggiungimento di un livello adeguato di sicurezza del sistema informatizzato richiede necessariamente alcuni adempimenti preliminari all'adozione delle concrete misure minime per garantire la sicurezza dei dati trattati, ed in particolare:

1. Individuazione degli elementi del sistema informatico che necessitano di protezione e delle minacce cui possono essere sottosposti (risorse hardware e software, banche dati, risorse professionali, Documentazioni cartacee, Supporti di memorizzazione)
2. Classificazione delle informazioni e delle banche dati trattate sulla base delle attività svolte, delle procedure operative adottate e della tipologia di trattamento effettuato (informazioni riservate, informazioni vitali per l'Amministrazione, ad uso interno, dati personali, dati sensibili, informazioni non classificate ecc.)
3. Applicazione di politiche di sicurezza, definite in base alla vigente normativa sulla sicurezza dei documenti informatici e dei dati personali, che comportino la definizione di un insieme di regole che fanno riferimento alle tecnologie utilizzate, alle modalità di trattamento e agli strumenti impiegati, agli incaricati del trattamento in base alla tipologia del dato ed alle conseguenze che la distruzione, l'alterazione o la perdita di riservatezza dei dati possono comportare.

1.1 Individuazione degli elementi del Sistema informativo comunale

L'organizzazione dei servizi comunali è articolata in 4 Settori a capo dei quali sono stati preposti dipendenti titolari di posizioni organizzative. Gli Uffici Comunali sono dotati di una rete informatizzata così articolata:

SEDI:

Sede Municipale, Piazza Vesi 6 Gatteo
Delegazione Comunale, Palazzo del Turismo, Piazza della Libertà Gatteo a Mare
Biblioteca ed Informagiovani

DOTAZIONE INFORMATICA:

⇒ N. 1 Server centrale HP 9000 MOD. 220: Si tratta di un server di rete già configurato e predisposto sia per il collegamento in architettura centralizzata, sia in LAN architettura Client – Server, dotato di una unità di backup ultraveloce di 2 Gb che permette l'effettuazione di copie automatiche più volte al giorno, consentendo la ripresa dopo un malfunzionamento hardware o software attraverso il ripristino del salvataggio effettuato. Il sistema è conforme ai principali protocolli di comunicazione (X25, TCP/IP7X400, ECC.) ed è in grado di supportare i più diffusi linguaggi di programmazione, database relazionali, strumenti per l'automazione d'ufficio ecc.

⇒ N. 1 Server Centrale Compaq: si tratta di un Server di rete configurato in architettura Lan Client – Server, dotato di unità di backup.

⇒ Tutti i PC sono stati collegati in rete LAN sia al Server Hp 9000 per la gestione di alcuni programmi comunali, sia al Server Compaq per l'autenticazione di rete, la posta elettronica ed il Programma di Protocollo ed atti.

⇒ La sede comunale di Gatteo e la delegazione di Gatteo a Mare sono state connesse via linea HDSL. La locale rete informatica è così composta:

- Una rete Lan locale a Gatteo a Mare che collega n. 5 Pc
- Una rete Lan locale a Gatteo che collega n. 37 Pc

⇒ I Pc collegati in rete Lan hanno la possibilità di condividere alcune risorse (FILE,DIRECTORY,CD,STAMPANTI ecct…),oltre all'accesso in LAN al server HP 9000 ed ai programmi comunali.

⇒ Il collegamento delle sedi di Gatteo e Gatteo Mare alla rete civica DELFO tramite Linea HDSL ha consentito il collegamento ad INTERNET di tutti i PC in rete LAN delle due sedi e la dotazione di indirizzi di posta elettronica per ogni Ufficio comunale. A tal scopo è stato registrato il dominio **comune.gatteo.fo.it**

⇒ La sicurezza del flusso di informazione è data dalla presenza presso il nodo di Cesena di FIREWALL, che garantisce da eventuali intrusioni esterne. Tuttavia, in ogni caso, tutte le informazioni on line relative al Comune di Gatteo sono posizionate nel server DELFO di Forlì. Pertanto, allo stato attuale, i PC della rete LAN e il server HP 9000 non sono accessibili o visibili dall'esterno.

PROCEDURE SOFTWARE:

La ditta Italsoft di Potenza Picena ha sviluppato per il Comune di Gatteo i seguenti applicativi: CONTABIL. FINANZIARIA , ESERCIZIO PROVVISORIO, ECONOMATO , GESTIONE PERSONALE, TRIBUTI, LEVA, ANAGRAFE , ELETTORALE, STATO CIVILE, SEGRETERIA, PROTOCOLLO, WORD PROCESSING, EDILIZIA, RETTE SCOLASTICHE, COMMERCIO. L'accesso a tali applicativi è possibile solo attraverso l'uso di password secondo un sistema modulato in base alle esigenze dei vari Uffici.

La Ditta Computer Center ha elaborato il programma Protocollo ed Atti, utilizzato a partire dalla metà del 2003. Tutto il software applicativo Computer Center è rispondente ad evoluti requisiti di Information Technology quali:

- rispetto degli standard
- completezza: copertura delle principali aree di un Ente Pubblico Locale
- impiego di protocolli di comunicazione e connessione a reti secondo gli standard ufficiali, quali TCP/IP per reti locali e geografiche Internet/Intranet
- integrazione con programmi di Office Automation come Microsoft Word e Microsoft Excel
- portabilità delle applicazioni su piattaforme hardware e sistemi operativi diversi
- interfaccia linguaggio HTML
- univocità delle informazioni
- interfaccia utente uniforme tra tutte le procedure, amichevole, di facile utilizzo e personalizzabile
- semplicità di installazione e di avviamento delle procedure
- facilità di accesso alle informazioni
- mantenimento "in linea" delle informazioni storiche dell'Ente
- collegabilità a banche dati e reti esterne sulla base degli standard ufficiali a livello comunitario e internazionale
- sicurezza operativa con personalizzazione degli accessi
- disponibilità di strumenti di personalizzazione potenti e facili da usare:
- funzionamento ottimizzato su architettura di tipo client/server in ambiente standard UNIX e WINDOWS

1.2 Classificazione delle Informazioni e delle banche dati trattate

L'Amministrazione Comunale disciplina tali aspetti attraverso:

- Atti Regolamentari che disciplinano l'organizzazione interna del Comune
- Manuale di Gestione del Protocollo Informatico
- Regolamento per la tutela della riservatezza delle persone e di altri soggetti rispetto al trattamento dei dati personali contenuti in archivi e banche dati comunali (Del. C.C. n. 75/1999)
- Identificazioni delle Banche Dati informatizzate e cartacee contenenti dati personali soggetti alla tutela della riservatezza ed individuazione dei Responsabili del trattamento (Del. G.C. n. 175/1999)
- Documento Programmatico sulla Sicurezza che definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali (Del. G.C. n. 164/2000).
- Provvedimenti dei Responsabili di Settore

1.3 Applicazione di politiche di sicurezza

Al fine di individuare ed applicare adeguate misure volte a garantire la sicurezza del sistema informativo, è compito dei Responsabili di Settore valutare, dinamicamente e costantemente:

- la vulnerabilità sia degli elementi costitutivi l'architettura del sistema informativo sia dei dati che in esso sono collocati;
- i rischi cui i dati sono soggetti.

A tale scopo si rilevano le seguenti minacce, a prescindere dall'origine dolosa, colposa o accidentale degli agenti che le possono generare:

⇒ distruzione documenti
⇒ perdita anche occidentale
⇒ accesso non consentito
⇒ trattamento non autorizzato

A tal fine devono essere predisposte delle misure minime di sicurezza:

1. Fisiche
2. logiche
3. organizzative

2. MISURE MINIME DI SICUREZZA

2.1 MISURE FISICHE

Il ruolo della sicurezza fisica è quello di proteggere i sistemi, le aree e le componenti del sistema informativo. Una adeguata protezione dei luoghi di lavoro serve a garantire la sicurezza dei dati custoditi al loro interno.

Per garantire questa sicurezza vanno adottate misure logistiche idonee ad assicurare la protezione di documenti, supporti informatici e apparecchiature rispetto al rischio di:

1. **accesso fisico non autorizzato;**
2. **distruzione o perdita dei dati dovuta ad eventi fisici.**

Verranno di seguito indicate le misure fisiche per assicurare :

1. **Sicurezza delle sale CED**
2. **Sicurezza delle postazioni di lavoro**

2.1.1 Sicurezza della sala ced

La Sala Ced del Comune di Gatteo è ospitato in due stanze limitrofe all'interno della sede comunale.

1. Protezione da accesso non autorizzato

Le stanze sono state dotate di sistemi antintrusione (porta d'ingresso blindata, porte di accesso chiuse a chiave e finestre con inferriate). Le chiavi di accesso alle sale server sono custodite da personale incaricato dal Responsabile del Settore Affari Generali. Il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri.
Per evitare il rischio di accesso fisico ai locali delle Sale Ced o l'intrusione da parte di persone non autorizzate si devono adottare le seguenti misure di sicurezza:

⇒ **Accesso di personale interno**

Possono accedere ai locali solo:

- Il Responsabile del Settore Affari Generali;
- Il referente informatico/amministratore del sistema laddove nominato;
- il custode delle chiavi;
- il personale che deve accedervi per l'espletamento dei compiti propri, per le necessità di gestione e manutenzione dei sistemi (ad es. il personale preposto al cambio giornaliero delle cassette di backup), dei locali e degli impianti nonché per attività di pulizia ed affini ed altre attività comunque indispensabili.

⇒ **Accesso di personale esterno**

Gli interventi di manutenzione o adeguamento sui server, sui locali che li contengono e sui relativi impianti, sono richiesti o comunque autorizzati dal Responsabile Settore Affari Generali o, laddove nominato, dall'Amministratore di sistema. Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno, vanno osservate le seguenti misure:

- il locale viene aperto dal personale custode delle chiavi;

- ciascun intervento è annotato su un apposito registro, conservato nella stanza del server, recante data e orario dell'intervento (inizio-fine), tipo di intervento, nome, cognome del tecnico intervenuto/Ditta o struttura, firma;
- al termine dell'intervento, l'incaricato della custodia della chiave provvede alla chiusura dei locali;
- nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal personale indicato nel paragrafo "Accesso del personale interno della struttura".

⇒ **Accesso di personale addetto alle pulizie**
- Non sussiste la necessità di effettuare quotidianamente le operazioni di pulizia nella stanza contenente il server: le giornate in cui il personale addetto alle pulizie accede alla medesima sono programmate, anche al fine dell'apertura del locale;
- è preferibile che le operazioni di pulizia si svolgano quando è presente il personale addetto alla custodia della chiave, che provvede personalmente all'apertura;ove non sia possibile la presenza del personale addetto alla custodia della chiave, in quanto l'intervento di pulizia si svolge al di fuori dell'orario di servizio o per altre cause ostative, in via eccezionale, il locale rimane aperto al fine di consentire l'ingresso del personale addetto, limitatamente ai periodi in cui è stato programmato l'intervento di pulizia;
- gli accessi sono registrati nell'apposito registro di cui sopra.

L'accesso alla sede comunale negli orari di chiusura degli Uffici sarà possibile a partire dal 2004 solo attraverso una smart card che consentirà l'identificazione delle persone in ingresso ed in uscita.

2. Distruzione o perdita dei dati dovuta ad eventi fisici

Tra gli eventi fisici che possono portare alla perdita dei dati per distruzione delle apparecchiature vengono considerati incendio, surriscaldamento delle apparecchiature, anomalie di alimentazione elettrica e altri eventi (allagamenti, crolli ecc.).

⇒ **Contromisure per rischio incendio**

Contro l'eventualità che un incendio nei locali in cui sono custoditi i sistemi server possa causare danni irreversibili ai dati, sono previste le seguenti misure di sicurezza:
- in prossimità del server è installato un dispositivo antincendio;
- le cassette di backup devono essere conservate in un armadio ignifugo, chiuso a chiave, dislocato in un locale diverso da quello che ospita il server.

⇒ **Contromisure per rischio danneggiamenti**

La chiusura della sala server garantisce la protezione delle apparecchiature da danneggiamenti accidentali o intenzionali.

⇒ **Contromisure per anomalie nell'alimentazione elettrica**

Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possa danneggiare i dati è stato predisposto un collegamento ad un gruppo statico di continuità.

2.1.2 Sicurezza delle postazioni di lavoro

1. Protezione delle postazioni di lavoro da accesso fisico non autorizzato

Per evitare il rischio di accesso fisico ai locali in cui vi sono uno o più postazioni di lavoro dotate di PC o l'intrusione da parte di persone non autorizzate si devono adottare le seguenti misure di sicurezza:

⇒ **Personale interno alla struttura**

- le postazioni di lavoro devono essere accessibili solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, di amministratori del sistema, o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili;
- l'accesso fisico ai luoghi di lavoro deve essere protetto tramite la presenza di personale ovvero tramite la chiusura delle vie di accesso;
- in ogni caso gli uffici aperti al pubblico devono essere presidiati da personale; negli orari diversi da quelle di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa.

⇒ **Personale esterno alla struttura**

la persona esterna può accedere ai locali solo quando è presente qualche addetto;

⇒ ***Assistenza con intervento in locale del tecnico***

Se sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc. presso la postazione di lavoro, è necessario che l'utente o il referente informatico o, in loro assenza altro dipendente della struttura, assista alle operazioni di manutenzione.

La segreteria deve trattenere e conservare copia del rapporto di intervento rilasciato dalla ditta intervenuta. Tale rapporto deve contenere data e orario dell'intervento (inizio e fine) descrizione sintetica del tipo di intervento, nome e cognome del tecnico intervenuto e della ditta, firma del tecnico e dell'utente che assiste all'intervento. Ove non già presenti nello schema, tali dati devono essere apposti dal personale di segreteria in presenza del tecnico intervenuto.

2. Protezione dei dati dal rischio di distruzione o perdita per eventi fisici

Gli eventi fisici che possono costituire fonte di rischio per le postazioni di lavoro sono quelli indicati nel paragrafo relativo ai server. Al fine di ridurre al minimo i rischi di distruzione o perdita di dati, è consigliabile:

- prediligere il lavoro sui dischi di rete, la cui protezione è assicurata dalle misure di sicurezza e di salvataggio automatico adottate per i server.
- In caso di utilizzo dei dischi installati fisicamente sul PC, vanno effettuati periodici backup dei dati su supporti magnetici, da conservare secondo quanto disposto nell'apposito paragrafo.

2.2 MISURE DI SICUREZZA LOGICHE

Per Sistema di sicurezza logica si intende il sottosistema della sicurezza finalizzato alla implementazione dei requisiti di sicurezza nelle architetture informatiche, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.

Ai sensi della vigente normativa, il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti specifiche tecniche:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'àmbito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Per il raggiungimento di tali obiettivi sono già state adottate alcune misure logiche che andranno rafforzate ed integrate al procedere dell'informatizzazione degli Uffici. I servizi di sicurezza logica attivati sono i seguenti:

- **Controllo Accessi**
- **Autenticazione**
- **Confidenzialità**
- **Integrità**

I Meccanismi di Sicurezza utilizzati, ovvero le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza sono i seguenti:

- **Meccanismi per il controllo degli accessi**
- **Meccanismi per l'autenticazione**
- **Controllo Instradamento**
- **Cifratura**
- **Meccanismi di salvataggio dati**
- **Antivirus**

Nel seguito vengono descritti i principali servizi e strumenti utilizzati.

2.2.1 Controllo degli accessi

Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico avvengano esclusivamente secondo modalità prestabilite.

Il controllo accessi viene visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione). Funzionalmente è costituito da:

- un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, modifica, cancellazione, esecuzione) secondo le quali i vari soggetti possono accedere agli oggetti;
- un insieme di procedure di controllo (meccanismi di sicurezza) che controllano se la richiesta di accesso è consentita o negata, in base alle suddette regole (validazione della richiesta)

2.2.2 Autenticazione

Per garantire quanto sopra esposto, il sistema informatico comunale è basato su un meccanismo che costringe ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ai programmi informatici comunali ed effettuare specifici trattamenti dei dati.

Ad ogni utente interno del Sistema Informativo Comunale è stato assegnata una credenziale di autenticazione, un codice identificativo personale costituito da nome utente e password, che consentono l'identificazione e l'accesso al proprio elaboratore ed alle risorse della rete. Ulteriori codici di identificazione personale sono stati attribuiti per consentire l'accesso ai programmi comunali installati sui Server di rete (Protocollo ed atti, Programmi Italsoft, Posta Elettronica, Antivirus). **Tutti i controlli sono svolti dal componente server**, anzichè sul meno sicuro client, ogni volta che si cerca di accedere ad un oggetto. E' possibile decidere quali "politiche" di sicurezza impostare: ad esempio definire i diritti d'accesso agli utenti a livello di singolo documento o creare profili d'accesso applicabili ai documenti in base alle proprietà e alle tipologie. A ciascun oggetto presente nel sistema possono venire associati diversi profili di accesso, stabilendo quali utenti o gruppi devono poter accedere e la tipologia di azione che questi possono compiere sull'oggetto stesso. Un utente può appartenere a diversi gruppi e si può decidere come gestire questa appartenenza multipla (assegnare permessi unione di tutti i permessi disponibili o permessi attualmente attivi in base alla sessione corrente).

2.2.3 Confidenzialità

Grazie al sistema di autenticazione sopradescritto, l'accesso ai documenti informatici ed il trattamento di dati personali con strumenti elettronici è consentito ai soli incaricati autorizzati a quello specifico trattamento.

Ogni utente autorizzato può accedere ad un'area di lavoro riservata per il settore o servizio di appartenenza, cui hanno diritto di accesso i soli componenti del gruppo di appartenenza. In questo modo l'operatore può:

- accedere alle risorse presenti fisicamente sulla macchina stessa (dischi fissi);
- accedere alle risorse di rete
- condividere con altri utenti risorse quali file, cartelle e stampanti;
- condividere con altri utenti applicazioni, quali ad es. Protocollo, Pratiche, ecc.;
- usufruire della centralizzazione delle operazioni di backup (nel caso in cui i dati siano salvati sul server) e di aggiornamento software.

Adempimenti

Ogni Responsabile di Settore, in collaborazione con il Referente Informatico, laddove nominato, deve predisporre soluzioni operative traduttive delle misure di sicurezza di tipo logico, volte a rafforzare quelle già esistenti, sulla base di un insieme di politiche e di regole di accesso che stabiliscono le modalità secondo le quali i vari soggetti possono accedere alle informazioni ed un insieme di procedure di controllo che verificano se la richiesta di accesso è consentita o negata in base alle suddette regole.

In particolare spetta ad ogni Responsabile di Settore con riferimento al proprio Settore:

1. Definire, in base alle competenze degli Uffici e dei Servizi del proprio Settore, per ogni incaricato del trattamento e per ogni banca dati quali tra le seguenti attività siano autorizzate:
   - Inserimento di dati
   - Lettura e stampa di dati
   - Variazione di dati
   - Cancellazione di dati
2. Assegnare ad ogni utente le credenziali di autenticazione sulla base delle attività autorizzate;
3. impartire le disposizioni operative per la sicurezza delle banche dati e del sistema di autenticazione, sulla base dei seguenti requisiti minimi:
   - ♦ Ogni nome utente è associato ad una ed una sola password, composta da almeno 8 caratteri, contenente elementi non riconducibili all'utente, conosciuta solamente dall'operatore e dal Referente Informatico, disabilitata qualora non sia più autorizzata.
   - ♦ Ogni utente deve adottare le necessarie cautele per assicurare la segretezza e la diligente custodia della password.
   - ♦ Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
   - ♦ In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
   - ♦ Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ad una specifica tipologia di dati. Tale verifica deve avvenire con cadenza annuale.
4. Definire le modalità con cui assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

2.2.4 Integrità fisica

Al fine di evitare i rischi di perdita dei dati informatici, temporanea o definitiva, e consentire il recupero di dati o file accidentalmente eliminati o erroneamente modificati, ovvero non disponibili per guasti hardware e software, limitando i disagi connessi con la discontinuità del servizio, è opportuno adottare una politica di backup sia sul server sia sulle postazioni di lavoro.

1. **Backup delle macchine server**

Tutti i dati dei sistemi informativi comunali ed i file utente presenti sui server centralizzati sono interessati da una politica di backup periodico su base giornaliera con controllo dell'avvenuto salvataggio. Il controllo viene effettuato da personale preposto allo scopo. Le letture dei supporti di backup avvengono in occasione delle richieste di ripristino di dati. I nastri vengono conservati in un armadio ignifugo in un locale separato.

Adempimenti

- il backup è gestito in automatico dal sistema server
- a livello della struttura sono presenti sei cassette magnetiche (DAT), una per ogni giorno della settimana (da lunedì a sabato), etichettate con il nome del giorno.
- La persona incaricata deve eseguire giornalmente le seguenti operazioni:
  - controllare, ogni mattina, tramite apposito programma l'esito del backup giornaliero:
  - contattare in caso di esito negativo del backup l'amministratore di sistema;
  - sostituire ogni mattina, sul sistema server, la cassetta magnetica contenete i dati di backup del giorno precedente con quella etichettata con il nome del giorno in corso;
  - collocare la cassetta contenente i dati di backup del giorno precedente in un locale diverso da quello in cui è dislocato il sistema server in armadi ignifughi chiusi a chiave; l'accesso agli armadi è consentito al solo personale autorizzato e deve essere protetto con misure di sicurezza fisiche non minori di quelle adottate per il server (in quanto le cassette contengono copia di tutti i dati presenti sul server);
  - provvedere alla manutenzione dell'unità nastro.

2. Backup delle postazioni di lavoro

Tutti i dati personali e sensibili presenti sulle postazioni di lavoro devono essere interessati da una politica di backup periodico su base mensile con controllo dell'avvenuto salvataggio.

2.2.5 Integrità logica

L'integrità logica si ottiene con il meccanismo di verifica dei privilegi di accesso ai file, garantito dal sistema operativo e con il sistema antivirus.

Contromisure:

Ogni utente, superata la fase di autenticazione, avendo accesso ai propri dati residenti nella propria area di lavoro, non può accedere alle altre aree né agli applicativi privo di autorizzazione. I virus sono particolari programmi, predisposti per essere eseguiti all'insaputa dell'utente, che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso.

Sul server Windows 2000 l'amministratore di sistema installa e provvede a mantenere un software antivirus con aggiornamento periodico automatico via Internet che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici. Il sistema antivirus risiede, oltre che sul server principale, sulle stazioni di lavoro utente.

2.2.6 Misure di sicurezza relative ad Internet

Le misure logiche di sicurezza devono inoltre estendersi al controllo del traffico di rete, al fine di garantire che la rete sia utilizzata esclusivamente dall'utenza autorizzata e nelle modalità definite dai profili di abilitazione.

Ogni computer collegato in rete può essere soggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete. Quando il computer è collegato a Internet le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in una qualsiasi parte del mondo.

Per fare fronte a questo rischio i posti di lavoro ed i server della struttura sono collegati alla rete Internet attraverso la rete Delfo, per cui la protezione dalla distruzione o perdita dei dati dovuta ad attacchi di malintenzionati, che agiscono collegandosi dall'esterno via Internet, è garantita dai sistemi gestiti dalla Provincia di Forlì-Cesena. Tra le principali misure di sicurezza per controllare l'accesso

alle reti su protocollo TCP/IP è di primario riferimento l'utilizzo di dispositivi firewall che sono in funzione presso il nodo di Cesena della rete Delfo.

Contromisure
Per difendersi dagli attacchi di questo tipo è opportuno tenere presente che:

- L'utilizzo di una connessione ad Internet (ad esempio via modem) attraverso un provider diverso da Delfo espone il PC utilizzato ai rischi normalmente presenti nel corso di una connessione ad Internet in assenza della protezione garantita da un firewall; l'eventuale attacco alla macchina nel corso della navigazione non protetta diventa in un fattore di rischio per l'intera rete provinciale;
- l'accesso a siti "impropri" e lo scaricamento di file non autorizzati in alcuni casi possono essere illegali e puniti dalla legge penale;
- l'utilizzo della connessione Internet per finalità non riconducibili all'attività di lavoro, anche se non produce un costo diretto, può diventare causa di sovraccarico della linea e può portare a un deterioramento della velocità della connessione per tutti gli utenti;
- le informazioni presenti su siti Internet non connessi a istituzioni conosciute possono essere non accurate, non valide o deliberatamente false: ogni decisione basata su di esse deve essere valutata adeguatamente;
- i messaggi di posta elettronica di cui non si conosce il mittente vanno trattati con la massima circospezione; non bisogna cliccare sugli eventuali allegati senza pensarci;

2.2.7 Misure di sicurezza relative ai supporti di memorizzazione

Nell'uso e nella conservazione dei supporti di memorizzazione si devono porre in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto e manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Inoltre, nel caso di reimpiego di supporti già utilizzati per il trattamento di dati sensibili o giudiziari, sono necessari gli ulteriori accorgimenti, di seguito riportati, derivanti dalle specifiche caratteristiche di tali supporti.

- possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili; altrimenti devono essere distrutti.

Nel caso in cui tali supporti siano consegnati a terzi, è opportuno rispettare le seguenti indicazioni:

- floppy disk e cd-rom riscrivibili: prima di essere consegnati ai terzi, debbono essere sottoposti ad una operazione di cancellazione delle informazioni precedentemente contenute con l'apposito comando di formattazione completa del supporto;
- hard disk: prima di essere consegnato ai terzi, deve essere sottoposto ad una operazione di cancellazione delle informazioni precedentemente contenute con il comando FDISK (che rimuove la partizione) e la formattazione della partizione successivamente creata;
- nel caso in cui, a seguito di intervento tecnico, si presenti la necessità di sostituire l'hard disk, è necessario procedere al recupero dei dati contenuti nello stesso, ove possibile e opportuno; dopo aver effettuato tale verifica si potrà procedere alla cancellazione dei dati dall'hard disk sostituito; si ricorda che l'hard disk potrebbe costituire un mezzo di esportazione illegittima di dati personali qualora gli stessi fossero recuperati da personale non autorizzato;

- nel caso in cui i supporti contenenti dati personali non siano destinati al riutilizzo essi debbono essere fisicamente distrutti mediante rottura.

2.3 MISURE ORGANIZZATIVE

2.3.1 Sicurezza Organizzativa

Gli aspetti organizzativi riguardano principalmente la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza e l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Sono già state poste in essere alcune misure, in particolare:

- Individuazione dei Responsabili del trattamento dei dati personali
- Adozione di un regolamento per la tutela della riservatezza (CC n.75 del 19.11.1997)
- Redazione e approvazione di un documento programmatico per la sicurezza

La realizzazione delle misure di sicurezza organizzative da implementare dovrà seguire il seguente piano:

- Individuazione di un responsabile di sistema con il compito di sovraintendere alle risorse del sistema operativo e che coordini l'effettiva adozione delle misure di sicurezza.
- Nomina di un Responsabile della tenuta del protocollo informatico , della gestione dei flussi documentali e degli archivi
- Istruzione interna e formazione secondo le schede allegate
- Adeguamento con cadenza annuale del piano programmatico per la sicurezza

2.3.2 Piano di formazione

La formazione dei dipendenti ha già coperto le seguenti problematiche:

- Utilizzo del software di gestione documentale Protocollo ed atti: modalità d'uso.
- L'accesso ad internet: Norme generali, Utilizzo corretto, Attivazione del servizio, Registrazione degli accessi:
- La posta elettronica: Norme generali, Utilizzo corretto, Attivazione del servizio
- La rete: Gli utenti di rete, Directory condivise, Monitoraggio e Gestione, Backup Centralizzato di rete, Utilizzo della rete
- Dovranno essere approfonditi i seguenti aspetti:
- Password: Modalità di assegnazione, gestione ed utilizzo, validità nel tempo.
- I virus informatici: Misure preventive, Regole operative, Norme sull'utilizzo dei programmi antivirus.
- Comportamenti illegali
- ·Norme disciplinari

Un ulteriore aspetto inerente la Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

E' stata creata una banca dati di tutte le dotazioni HW, SW e di trasmissione dati.

Questo archivio viene tenuto aggiornato con le sostituzioni e fornisce una visione storica e precisa del patrimonio; è di aiuto nei processi di acquisto ed in quelli di pianificazione degli investimenti e delle scorte e materiali di consumo.

Allegato 6: Abilitazione all'utilizzo del Sistema di gestione informatica dei documenti, livelli di riservatezza e corrispondenti logiche di protezione

In questo allegato sono descritte le abilitazioni all'utilizzo del sistema di gestione informatica resi possibili dal programma Protocollo ed Atti, i livelli di riservatezza applicabili ai documenti registrati al protocollo e per ciascun livello di riservatezza, le relative abilitazioni all'accesso al patrimonio informativo e documentale.

Il Sistema di gestione documentale "Protocollo ed atti" consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti, in condizioni di sicurezza nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. L'accesso alle informazioni è sicuro e personalizzabile, conformemente alle esigenze dell'Ente e del tipo di utente. E' possibile decidere quali "politiche" di sicurezza impostare: ad esempio definire i diritti d'accesso agli utenti a livello di singolo documento o creare profili d'accesso applicabili ai documenti in base alle proprietà e alle tipologie. A ciascun oggetto presente nel sistema possono venire associati diversi profili di accesso, stabilendo quali utenti o gruppi devono poter accedere e la tipologia di azione che questi possono compiere sull'oggetto stesso.

Accesso al programma:
Nel caso concreto del Comune di Gatteo, l'accesso all'applicazione da parte degli utenti avviene attraverso un semplice ed efficace sistema di protezione, basato su un meccanismo di autentificazione individuale. Ad ogni utente interno del Sistema Informativo Comunale è stato assegnata una credenziale di autenticazione, un codice identificativo personale costituito da nome utente e password, che consentono l'identificazione e l'accesso al programma. Tutti i controlli sono svolti dal componente server, anzichè sul meno sicuro client, ogni volta che si cerca di accedere ad un oggetto.

Definizione di Ruoli Funzione:
Attraverso una specifica parte del programma, l'Amministratore del Sistema, in collaborazione con i Responsabili di Settore, definisce i "Ruoli Funzione" : tale funzione consente di creare liste di utenti abilitati, perché inseriti nell'elenco degli elementi presenti, ad assolvere alle funzioni assegnate, attraverso la selezione di specifiche funzionalità, scelte tra quelle disponibili. Alcuni ruoli funzione sono prestabiliti, ma è consentita la definizione di nuovi ruoli anche al di fuori di quelli previsti nelle strutture organizzative e politiche, al fine di rendere più flessibile l'assegnazione dei permessi. L'operatore ha a disposizione un elenco di funzioni che definiscono azioni specifiche, attivabili in presenza dei moduli operativi a cui si riferiscono. L'assegnazione di opportune funzionalità a specifici profili, consente l'abilitazione degli utenti indicati a quel ruolo.

Definizione di Ruoli permessi:
L'assegnazione di un ruolo permesso definisce i permessi d'accesso ai documenti, individuando gli elementi presenti tra gli uffici competenti dell'Ente e il personale abilitato. Nella vista, per ciascun ruolo permesso, viene riportato la descrizione assegnata e l'elenco delle persone inserite. La selezione della descrizione del ruolo permesso, fa accedere al modulo in cui sono impostati i dati.

Nel caso del modulo di protocollo sono stati definiti i seguenti Ruoli Funzione e Ruoli permessi:

1. **"Gestore ADM":** Amministratore del sistema; superutente che ha pieni diritti sul sistema;

2. **"Gestore globale":** Consente il pieno controllo sulle funzioni "amministrative" del sistema di gestione documentale.

Ruoli permessi:Funzionari autorizzati	Elenco Funzioni Amministrazione
Responsabile Settore Affari generali Referente Informatico Amministratore di sistema	Gestione organigramma operativo Visualizza dettaglio operativo Visualizza storico Elimina funzionario\UO Gestione organigramma Politico Visualizza dettaglio politico Visualizza storico Elimina amm.re\OC Gestione altre anagrafiche Elimina soggetti\categorie Gestore documenti Gestore titolario Gestore schemi documenti Gestore nuova classe nel titolario Gestore procedimenti Gestore schemi procedimenti Gestore protocollo Gestore protocollo chiuso Gestore ufficio protocollo Richiedi statistiche Pubblica statistiche Gestore stampe

3. "**Gestore protocollo":** Consente il pieno controllo sul modulo di protocollazione dei documenti

Ruoli permessi:Funzionari autorizzati	Elenco Funzioni Amministrazione
Responsabile Settore Affari generali Responsabile Protocollo Addetti Autorizzati dal Responsabile Protocollo Referente Informatico	Gestione organigramma operativo Visualizza dettaglio operativo Visualizza storico Gestione altre anagrafiche Elimina soggetti\categorie Gestore documenti Gestore titolario Gestore schemi documenti Gestore nuova classe nel titolario Gestore protocollo Gestore protocollo chiuso Gestore ufficio protocollo Protocolla documenti e atti Gestore albo pretorio Gestore stampe

4. **"Gestore documenti":** E' la tipologia di utente che ha accesso al programma di protocollazione dei documenti soltanto attraverso la procedura di creazione del documento informatico. Tale utente può creare un protocollare un documento in partenza, e può accedere in lettura al

programma del protocollo, ma non può protocollare documenti in uscita né apportare modifiche alle registrazioni di protocollo dei documenti di cui non è l'autore.

Ruoli permessi:Funzionari autorizzati	**Elenco Funzioni Amministrazione**
Tutti gli utenti interni del sistema informativo	Elimina soggetti\categorie Gestore documenti Gestore titolario Gestore schemi documenti Gestore proposta Gestore schemi e tipi su atti decisionali Gestore seduta Gestore albo pretorio Gestore contratti Gestore stampe

{PRIVATE "TYPE=PICT;ALT="**}**

⇒ **COME AVVIENE L'INSERIMENTO DI UN NUMERO DI PROTOCOLLO:**

Il corretto inserimento prevede l'assegnazione di anno e numero protocollo. La numerazione dei documenti protocollati è strettamente progressiva e viene assegnata automaticamente dalla procedura al termine delle operazioni di inserimento.

Viene inoltre richiesta la data di registrazione, la segnatura se in entrata o in uscita, la lista degli intestatari con richiesta della ragione sociale dei mittenti/destinatari, a seconda che il protocollo sia in entrata o uscita, con indirizzo completo ed eventuali note di comunicazione dell'intestatario, e l'oggetto del protocollo.

L'assegnazione dell'Unità organizzativa e del responsabile non è obbligatoria ma consigliabile. Il sistema, in fase di inserimento, nel caso non vengano assegnati i valori, richiede conferma prima di procedere. L'operatore può tenere indicazione degli eventuali protocolli antecedenti o susseguenti, in modo da mantenere un collegamento, impostare uno schema protocollo tra quelli disponibili, assegnare la classificazione nel Titolario d'archivio indicando Categoria, Classe, Fascicolo e Materia di riferimento e riportare gli estremi del documento originale. Può inoltre indicare gli estremi del Procedimento, se è presente il modulo di gestione dei Flussi Documentali.

Sul protocollo è possibile allegare un file sia come "documento informatico" (definizione di legge in cui un documento elettronico è firmato digitalmente secondo lo standard P7M) sia altro documento. Se il documento è "documento informatico" deve essere presente la sua verifica e calcolo della segnatura attraverso l'integrazione con il prodotto DigitalSign di CompEd.

Per la sicurezza dei documenti del tipo "Protocollo", l'operatore ha la possibilità di assegnare gli accessi in modifica ossia gli autori.

RENDI RISERVATO:
La funzione permette di assegnare diritti di visione ad un particolare utente o gruppo di utenti, rendendo di fatto riservato il protocollo.
L'utente ha la possibilità di eliminare eventuali utenti o gruppi di utenti già presenti negli accessi in lettura attraverso il pulsante "Elimina", oppure di introdurne dei nuovi attraverso il pulsante "Aggiungi". Ad operazione ultimata viene ricaricata la lista dei protocolli; il protocollo reso riservato è individuabile attraverso l'apposita icona.

ALLEGATO 7: PROGETTO PANTA REI

PRESENTAZIONE

Il progetto Panta Rei ha la finalità di costruire un network territoriale a scala provinciale fra le amministrazioni Pubbliche per la circolazione digitale della documentazione al fine di realizzare servizi innovativi per i cittadini e per le imprese. In una prima fase lo scopo è limitato al miglioramento del livello di automazione dei processi di comunicazione nella pubblica amministrazione. In una seconda fase i servizi verranno estesi, allo scopo di migliorare i servizi ai cittadini e alle imprese.

Le finalità del progetto Panta Rei comprendono:

- potenziare l'infrastruttura di rete telematica provinciale (già esistente) ed implementare tecnologie e servizi che abilitino la comunicazione digitale e lo svolgimento on line dei procedimenti amministrativi, anche attraverso la modalità del telelavoro, sia tra Amministrazioni che da Amministrazione a cittadino/impresa ;
- finalizzare l'infrastruttura tecnologica ed i servizi, di cui al punto precedente, alla relazione fra P.A. ed Imprese favorendo la crescita di "Sportelli Virtuali per l'Impresa" ma non trascurando di supportare con forza la rete esistente degli Sportelli Unici per le Imprese così da favorirne il rilancio;
- estendere i servizi generali e specifici ottenuti alla rete degli URP degli Enti.

Il progetto necessita di una forte componente INFRASTRUTTURALE per garantire:

- **Sistemi sicuri**
- **Protocollo informatico a norma + una piattaforma documentale di riferimento**
- **Firma digitale**
- **Archiviazione documenti a norma**

E' necessario quindi organizzare e condividere un modello di Servizi generali (infrastrutturali o di piattaforma):

- ✓ Gestione della documentazione elettronica in formazione
- ✓ Gestione della documentazione elettronica finita a norma: registrazione di protocollo, gestione dei procedimenti
- ✓ archiviazione sostitutiva,
- ✓ Attivazione di forme di telelavoro
- ✓ Cooperazione ed interoperabilità: posta sicura, time stamping, accessi condivisi in sicurezza
- ✓ Interazione esterna: attivazione telematica, consultazione on line, notifica eventi, restituzione esito finale

Polo Territoriale

Nell'ambito di ogni territorio provinciale si realizza un Polo territoriale attrezzato, sotto il profilo hardware e software. I Poli territoriali provvedono alla gestione dell'archiviazione - a norma - della

documentazione elettronica. Ogni amministrazione è collegata al polo Territoriale e fruisce dei servizi generali proposti.

Attività svolte nel 2002

- ✓ Presentazione progetto entro i termini stabiliti (primi di Giugno).
- ✓ L'approvazione del progetto ha avviato il processo di perfezionamento degli accordi con tutti i partner.
- ✓ Sono stati approvati entro l'anno tutti gli schemi di convenzione presso i rispettivi Consigli Provinciali.
- ✓ Si è avviato il processo tecnico.In particolare è stato perfezionato l'accordo con il partner tecnologico (Hummingbird) ottenendo condizioni economiche estremamente vantaggiose.
- ✓ Si è infine mantenuto attivo il coordinamento fra le Province di Bologna e fra ogni Provincia per diffondere nelle strutture la conoscenza e la piena consapevolezza del progetto Panta rei.

Obiettivi e risultati attesi per il 2003/2004

- ✓ Coordinamento delle azioni sui territori e coinvolgimento tecnico/operativo dei Comuni nella progettazione.
- ✓ Rilevazione delle architetture tecnologiche di riferimento.
- ✓ Acquisizione licenze EDMS.
- ✓ Definizione delle specifiche comuni di progetto (per le applicazioni verticali di protocollo);
- ✓ Progettazione esecutive riferite alle architetture dei poli ed avvio delle gare di fornitura, in particolare server per piattaforma EDMS;
- ✓ Specifiche per sistema di autenticazione, di firma digitale e di posta certificata, per sistema di AOS ed avvio gara per approvvigionamento;
- ✓ Completamento dell'approvvigionamento ed avvio delle implementazioni dei poli;
- ✓ Avvio processo di accreditamento dei fornitori (già terminata la prima fase);
- ✓ Manuale di gestione tipo da porre in uso presso gli enti dal 1/1/2004;
- ✓ Realizzazione delle integrazioni sui sistemi verticali di protocollo;
- ✓ Elaborazione specifiche di progetto per la realizzazione dei servizi tipo.
- ✓ Enti con protocollo a norma integrato con EDMS;
- ✓ Allestimento del Polo territoriale in termini di hardware e software di base (ad esclusione del sistema AOS) per il 60% delle Province in sviluppo;

COSA SUCCEDERA' A BREVE NEGLI ENTI COINVOLTI :

La Provincia renderà disponibile a tutti gli Enti alcune strumentazioni e tecnologie basilari:

1. Un apparecchio SCANNER per poter acquisire documenti cartacei;
2. Un numero adeguato di certificati di firma digitale (per Dirigenti/Funzionari, etc)
3. Un numero adeguato di LETTORI SMART CARD
4. Un numero adeguato di SMART CARD
5. Un SW per gestire le delle SMART CARD e API
6. Un congruo numero di licenze HUMMINGBIRD (licenze client)
7. Una licenza HUMMINGBIRD server

Inoltre la provincia realizzerà un polo tecnologico territoriale inserendo nuovi Server e/o potenziando gli attuali, attrezzandoli con DBMS e i SW necessari per garantire la funzionalità del modello. Inoltre, solo per gli Enti aderenti a Pantarei che hanno un fornitore SW di protocollo accreditato (vedi elenco) la Provincia garantirà la copertura finanziaria necessaria (con gli importi come stabilito in convenzione con il capo progetto Pantarei) a garantire il rilascio del SW di protocollo a norma AIPA (T.U. 445/2000) e conforme alle specifiche Pantarei

COSA DEVONO FARE GLI ENTI COINVOLTI :

⇒ Devono collaborare attivamente con la struttura di polo territoriale per produrre un modello cooperativo e organizzativo soddisfacente e funzionale (partecipazione a gruppi di lavori locali);

⇒ Essere disponibili a rivedere alcune metodologie organizzative se in contraddizione con i nuovi modelli;

⇒ Adeguarsi agli obblighi di legge (come previsto nel DPR 445/2000)

⇒ Collaborare attivamente nella sperimentazione (necessaria, almeno in una prima fase del progetto);

⇒ dedicare alcune risorse economiche del 2003/2004 per sostenere i costi (servizi) necessari all'attivazione dei nuovi programmi di protocollo e per favorire il decollo al nuovo sistema.

COMPONENTI TECNOLOGICHE DEL PROGETTO

Si descrivono nel seguito alcuni dettagli di alto livello relativamente all'infrastruttura e all'architettura delle componenti tecnologiche previste nell'ambito del progetto Panta Rei.

⇒ Infrastruttura tecnologica prevista

Allo scopo di raggiungere gli obbiettivi di progetto, è necessario procedere all'acquisizione di componenti sia di servizi applicativi sia infrastrutturali:

Le componenti applicative comprendono:

- Electronic Document Management (EDMS);
- Protocollo Informatico.

Le componenti infrastutturali comprendono:

- Posta elettronica certificata;
- Gestione utenze e autenticazione;
- Firma digitale.

Si precisa a questo riguardo che:

- La piattaforma di Document Management è già stata identificata e selezionata nel prodotto HummingBird. Tale piattaforma è a fattor comune tra tutti gli enti aderenti al progetto Panta Rei.
- La piattaforma di gestione del protocollo non è soggetta a vincoli di omogeneità tra enti. Non verrà selezionata una piattaforma, nè un fornitore singolo. Ogni ente rimane libero nell'identificazione del fornitore e del prodotto, fatta salva l'apertura all'integrabilità con le altre componenti previste dalla conformità alle caratteristiche tecniche, definite dal comitato tecnico del progetto Panta Rei.
- L'infrastruttura di posta certificata verrà acquisita come servizio da uno dei fornitori italiani iscritti al registro fornitori PEC-AIPA. Non si prevede quindi alcuna acquisizione di hardware e software specifico per una installazione gestita in autonomia.
- L'infrastruttura di autenticazione sarà basata su Directory Server Standard LDAP V.3.

⇒ **Attori**

Gli aderenti alla prima fase di progetto Panta Rei sono enti della Pubblica Amministrazione di due tipologie:

- **Poli territoriali**: Province o Comuni di grande dimensione sul territorio Italiano, che si doteranno delle necessarie infrastrutture per l'erogazione di servizi ad uso interno e per l'erogazione a enti esterni via interfaccia Web.
- **Satelliti**: Enti quali comuni di dimensioni medio/piccole utilizzatori di servizi resi disponibili dal polo territoriale di appartenenza.

⇒ **Macro Architettura del sistema**

I Poli Territoriali saranno dotati di una istallazione autonoma del sistema di Electronic Document Management (EDMS). La stessa installazione verrà utilizzata sia per uso interno sia per l'uso da parte degli enti satelliti del territorio di competenza.

Ciascun Polo Territoriale e ciascun Satellite sarà dotato di applicativi di Protocollo Informatico conformi alla normativa AIPA e approvati dal comitato tecnico Panta Rei[1].

Sia il prodotto di EDMS sia i prodotti di Protocollo si avvarranno di Directory Server LDAP per l'autenticazione degli utenti. In particolare, nell'ambito di uno stesso Polo Territoriale, i servizi di EDMS e di Protocollo utilizzeranno lo stesso Directory server per l'autenticazione degli utenti.

Non è previsto alcun grado di integrazione, né tra Poli Territoriali distinti né tra satelliti appartenenti a poli diversi, se non a mezzo di comunicazioni via posta elettronica certificata. In questo senso quindi il progetto prevede la costruzione di più Poli Territoriali inter-indipendenti, ciascuno dei quali dotato di un ente centrale e più enti satellite, in cui la totalità degli utenti è censita in un unico directory server, utilizzato da una istanza di EDMS e da più istanze di Protocollo (vedi Fig. 1).

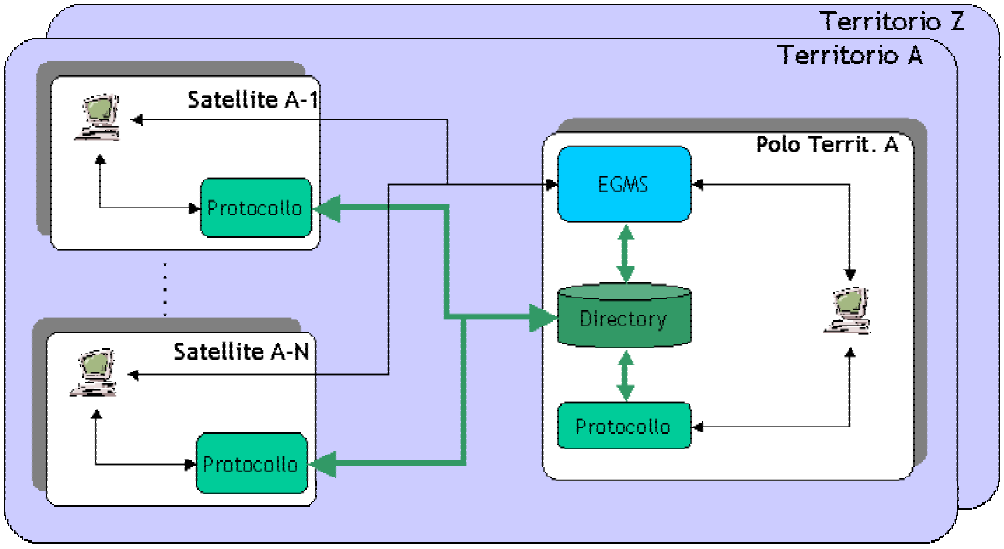

Fig. 1 Macro Architettura del sistema

Come accennato in precedenza, uno degli scopi del progetto è quello di centralizzare l'autenticazione degli utenti nell'ambito di un unico directory server LDAP nell'ambito di ciascun Polo territoriale.

Note tecniche relative alla infrastruttura per la firma digitale

La fornitura dovrà essere in linea con il quadro normativo italiano ed europeo:

- Legge 15 marzo 1997, n.59 (in Suppl. ordinario n. 56/L, alla Gazz. Uff. n. 63, del 7 marzo). Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa
- Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Gazz. Uff. n. 60 del 13 marzo 1998). Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59.
- Decreto del Consiglio dei Ministri 8 febbraio 1999 (Gazz. Uff. n. 87 del 15 aprile 1999). Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513.
- CIRCOLARE CR/22, 26 luglio 1999 (Gazz.Uff. 2 agosto 1999, Serie Generale, n. 179) Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Modalità per presentare domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.
- Direttiva 1999/93/CE, 13 Dicembre 1999
- CIRCOLARE n. AIPA/CR/24, 19 giugno 2000 (G.U. 30 giugno 2000, Serie generale n. 151) Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Gazz. Uff. n. 42 del 20 febbraio 2001). Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- CIRCOLARE n. AIPA/CR/27, 16 febbraio 2001 Art. 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni.
- Decreto legislativo 23 gennaio 2002, n. 10 (Gazz. Uff. n. 39 del 15 febbraio 2002). Recepimento della Direttiva 1999/93/CE sulla firma elettronica.
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137 (Gazz. Uff. n.138 del 17 giugno 2003). Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n.10.

⇒ **Macro requisiti**

Gli enti aderenti al progetto Panta Rei non sono attualmente dotati di certificati ad uso Firma Digitale. Si vogliono dotare tutti i dipendenti delle pubbliche amministrazioni coinvolte nel progetto Panta Rei di certificati elettronici qualificati per la firma digitale avanzata, cioè per la firma con validità legale. Ogni dipendente dovrà essere dotato di una smart card, che costituisce il dispositivo di firma, all'interno della quale deve essere generata e custodita la chiave privata utilizzata per il processo di firma digitale. I certificati digitali dovranno in futuro poter essere memorizzati anche all'interno di carte CIE (Carta d'Identità Elettronica) e CNS (Carta Nazionale dei Servizi). Oltre alle smart card, saranno forniti i relativi lettori/scrittori di smart card, che risultino ovviamente compatibili con le smart card stesse, ed il software necessario all'interfacciamento di questi dispositivi hardware con i pc.

⇒ **Smart card**

Le smart card dovranno essere dotate di coprocessore crittografico (smart card crittografiche) e possedere almeno le seguenti caratteristiche funzionali e tecniche:

- generazione delle coppie di chiavi;
- memorizzazione e gestione di più chiavi private e certificati (qualificati e non);
- effettuazione delle operazioni per la firma digitale;
- effettuazione delle operazioni per la cifratura e decifratura;
- compatibilità con standard ISO 7816-1/2/3/4 (T=0, T=1);
- generatore chiavi RSA 1024 bit a bordo (come previsto dalla norma);
- memoria dati non inferiore ai 32 Kbyte;
- componente hardware (chip) con certificazione di sicurezza.

La smart card sarà utilizzabile solo attraverso PIN di accesso, modificabile liberamente dall'utente, e non più utilizzabile dopo un certo numero di tentativi di immissione del PIN falliti. Deve essere disponibile inoltre la funzione di sblocco attraverso codice (PUK), fornito all'utente insieme al PIN.

Le *smart card* ed il software forniti dovranno essere:

- in grado di interagire con il più ampio insieme di *client* di e-mail comunemente diffusi sul mercato (Outlook, Eudora, Lotus, GroupWise, ecc.) al fine di consentire operazioni di firma, cifratura, verifica della firma e decifratura su messaggi di posta elettronica;
- integrabili nei principali prodotti di office automation (Microsoft Office, Acrobat, ecc.);
- integrabili con i principali browser web (Microsoft Internet Explorer, Netscape);
- compatibili con i sistemi operativi Microsoft per l'automazione del login sia a reti Microsoft sia a reti Novell (quindi con eventuale presenza del client Netware).

⇒ **Lettori**

I lettori dovranno possedere almeno le seguenti caratteristiche tecniche:

- lettori/scrittori di tipo esterno;
- totale compatibilità con le *smart card* richieste (e descritte nel punto precedente);
- connessione per trasferimento dati di tipo PS/2;
- connettore di alimentazione passante per porta PS/2;
- compatibilità driver PC/SC;
- compatibilità con i sistemi operativi: MS Windows 95, 98, Me, NT4, 2000, XP;

I lettori devono consentire le funzionalità di scrittura sulla smart card ed il software necessario a svolgere tale attività.

⇒ **Servizi di certificazione e certificati**

Dovrà essere garantita la fornitura del servizio di *Certification Authority* (CA) per certificati qualificati (certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondano ai requisiti fissati dall'allegato II della medesima direttiva). Verrà assicurata la gestione dell'intero ciclo di vita dei certificati digitali, cioè:

- emissione nuovi certificati;
- gestione delle revoche e delle sospensioni dei certificati;
- distribuzione e pubblicazione dei certificati e delle liste dei certificati revocati (CRL) o sospesi (CSL);
- le liste devono essere disponibili e consultabili in modo continuativo, come previsto dalla normativa vigente, attraverso protocollo LDAP/LDAPS, presso un sito comunque controllabile dagli utenti;
- le CRL e CSL devono essere disponibili agli utenti per mantenere le informazioni a loro disposizione aggiornate;

- rinnovo dei certificati;
- archivio dei certificati emessi dalla CA;
- servizi di *logging*;
- servizi di *backup* e *recovery*.

E' prevista la fornitura di certificati qualificati per firma avanzata, cioè firma elettronica ottenuta attraverso una procedura informatica che garantisca la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. La validità dei certificati deve essere al massimo di tre anni.

⇒ **Certificati per autenticazione interna**

Nell'ambito del progetto è prevista anche la fornitura di certificati a uso della realizzazione di politiche di strong authentication sui sistemi interni.

⇒ **Servizi di registrazione**

E' prevista la definizione di più *Local Registration Authority* (LRA) presso i singoli poli territoriali.
Non è attualmente definito il numero di LRA previste. Tale numero potrebbe anche essere zero nel caso in cui si decidesse di avvalersi della rete sul territorio del certificatore per la distribuzione dei certificati. In ogni caso, data la natura distribuita sul territorio del progetto Panta Rei, è di particolare interesse la flessibilità del modello di distribuzione realizzabile tramite LRA.

Si descrive nel seguito il modello preferenziale identificato dal comitato tecnico:

1. Ciascun polo territoriale nominerà una o più persone incaricate del processo di emissione e distribuzione delle smart card contenenti i certificati.
2. Gli incaricati potranno avvalersi di un qualsiasi PC dotato di Browser (e ovviamente di card reader/writer) senza ulteriori requisiti oltre a tipo e versione del browser stesso o presenza di plug in scaricabili da rete.
3. Gli incaricati potranno generare più smart card con certificati in autonomia, senza la compresenza del destinatario della Smart Card.
4. La consegna delle card ai destinatari, previa identificazione, può avvenire senza alcuna dipendenza da PC connessi o meno in rete.

⇒ **Servizio di time stamp**

Il servizio di time stamp dovrà permettere di attestare in modo certo l'esistenza di un documento informatico ad una certa data ed a una certa ora. Deve essere infatti possibile stabilire la collocazione temporale del documento stesso e della firma digitale su di esso apposta, al fine di evitare che un documento elettronico venga firmato con una chiave privata relativa ad un certificato che abbia esaurito il proprio periodo di validità, oppure che sia stato revocato.Il servizio dovrà generare, a fronte di una richiesta esplicita, una marca temporale, cioè un messaggio firmato digitalmente dalla autorità di validazione temporale utilizzando una chiave privata dedicata esclusivamente alla sottoscrizione di marche temporali. Le informazioni contenute nelle marche temporali emesse devono essere conformi a quelle definite dalla normativa. Il servizio deve includere anche la gestione di meccanismi di *logging* e *auditing* e di archiviazione delle informazioni riguardanti le richieste di marche temporali.

⇒ **Software di firma e verifica**

E' prevista la fornitura di un software per effettuare le operazioni di firma e di verifica della firma stessa. Il sistema dovrà fornire (sia direttamente agli utenti sia alle applicazioni che ne utilizzano i servizi) le seguenti funzionalità:

- firma digitale avanzata
- verifica firma;
- servizio di time stamp

Il sistema dovrà rispettare eventuali specifiche derivanti dalle normative vigenti riguardanti la firma digitale e i documenti in formato informatico. Qualora si verifichino variazioni normative, il fornitore sarà tenuto ad apportare le necessarie modifiche. I client installati nelle varie postazioni devono essere in grado di effettuare le operazioni di firma e verifica. Per quanto riguarda l'apposizione della marca temporale, il client deve interagire con il server di time stamping che rilascia la marca temporale richiesta e firma il documento marcato temporalmente.

⇒ **Firma digitale**

Per le funzionalità di firma digitale, attraverso il client l'utente potrà essere in grado di firmare documenti residenti sul proprio computer ottenendo risultati nei formati standard, in particolare quelli previsti dalla normativa vigente. Sarà possibile l'apposizione di firma di tipo attached e di tipo detached. Il client potrà utilizzare certificati differenti residenti nella stessa smart card.

⇒ **Verifica firma**

Attraverso il client, l'utente dovrà avere la possibilità di verificare firme di tipo attached e detached. Il processo di verifica di una firma ritorna all'utente il relativo risultato, il file originale e le informazioni contenute nei campi del certificato utilizzato per firmare il file verificato. Il livelli di verifica previsti sono i seguenti:

1. verifica di integrità;
2. verifica di credibilità con controllo del certificato di CA che ha rilasciato il certificato utilizzato;
3. verifica di validità con controllo delle CRL e CSL.