



Manuale di gestione
del Protocollo Informatico
dei documenti e dell'archivio

Unione Territoriale Intercomunale
del Torre

Registro delle versioni

N. Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
0.0	Maggio 2018		Approvato con atto UDP n. 20/2018

Unione Territoriale Intercomunale del Torre



INDICE

1. PRINCIPI GENERALI	
1.1. Premessa	3
1.2. Ambito di Applicazione	3
1.3. Norme di riferimento e definizioni	3
1.4. Modello organizzativo	4
1.5. Aree Organizzative Omogenee	4
1.6. Accreditamento dell'AOO all'IPA	4
1.7. Servizio per la gestione informatica del protocollo	5
1.8. Caselle di Posta elettronica	5
2. CARATTERISTICHE DEL PROTOCOLLO INFORMATICO	
2.1. Unicità del protocollo informatico	5
2.2. Registro giornaliero di protocollo	6
3. DOCUMENTO	
3.1. Formazione del documento amministrativo analogico	6
3.2. Formazione del documento amministrativo informatico	6
3.3. Documento in arrivo	7
3.4. Documento in partenza	7
3.5. Documento interno	7
4. DESCRIZIONE DELLA LAVORAZIONE DEL FLUSSO DOCUMENTALE IN ARRIVO	
4.1. Ricezione dei documenti informatici	7
4.2. Ricezione dei documenti cartacei a mezzo posta convenzionale	8
4.3. Ricezione e trasmissione di documenti cartacei a mezzo fax	8
4.4. Fatture, assegni e altri valori di debito o credito	8
4.5. Protocollazione di documenti inerenti gare di appalto confezionate su supporto cartaceo	9
4.6. Protocolli urgenti	9
4.7. Documenti non firmati – anonimi	9
4.8. Messaggi di posta elettronica pervenuti nelle caselle e-mail sei singoli dipendenti	9
4.9. Integrazioni documentaria	9
4.10. Documenti indirizzati nominalmente al personale dell'U.T.I. del Torre	10
4.11. Protocollazione di un numero consistente di documenti cartacei	10
4.12. Interoperabilità dei sistemi di protocollo informatico	10
4.13. Registrazione e segnatura di protocollo dei documenti ricevuti	10
4.14. Livello di riservatezza	11
4.15. Errata ricezione dei documenti analogici	11
4.16. Errata ricezione dei documenti digitali	11
4.17. Rilascio di ricevute attestante la ricezione di documenti informatici	11
4.18. Rilascio di ricevute attestante la ricezione di documenti cartacei	11
4.19. Elementi facoltativi delle registrazioni di protocollo	12
4.20. Termini per la registrazione di protocollo	12
4.21. Differimento dei termini di registrazione	12
4.22. Annullamento delle registrazioni di protocollo	12
5. REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI	
5.1. Regole generali	12
5.2. Regole disponibili con il Sistema di Protocollazione -SdP	13
5.3. Attività di assegnazione	13
5.4. Assegnazione dei documenti ricevuti in formati digitale	13
5.5. Assegnazione dei documenti ricevuti in formato cartaceo	13
5.6. Modifica delle assegnazioni	14
6. GESTIONE DELLA CORRISPONDENZA IN PARTENZA	
6.1. Trasmissione dei documenti	14
6.2. Spedizione dei documenti su supporto cartaceo	14

Unione Territoriale Intercomunale del Torre



7.	ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	
7.1.	Documenti non soggetti a registrazione di protocollo	15
7.2.	Documenti soggetti a registrazione particolare	16
8.	REGISTRO DI EMERGENZA	
8.1.	Il Registro di Emergenza	16
8.2.	Modalità di apertura del registro di emergenza	16
9.	ACCESSO AL SISTEMA	
9.1.	Abilitazione per l'accesso all'uso del SdP-GIFRA	16
9.2.	Abilitazioni	17
9.3.	Utenti esterni alla AOO da parte di altre Pubbliche Amministrazioni	17
9.4.	Utenti esterni alla AOO – Privati	17
10.	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE	
10.1	Classificazione dei documenti	17
10.2	Fascicolazione dei documenti	18
11.	CONSULTAZIONE, MOVIMENTAZIONE dell'archivio corrente, di deposito, storico e CONSERVAZIONE	
11.1	Principi generali	18
11.2	Consultazione ai fini giuridico-amministrativi	18
11.3	Consultazione da parte di utenti interno all'AOO	19
11.4	Consultazione da parte di utenti esterni all'AOO	19
11.5	Diritto di accesso e tutela dei dati personali	19
11.6	Scambio di documenti all'interno dell'AOO	20
11.7	Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei Documenti cartacei	20
11.8	Conservazione dei documenti informatici	20
11.9	Piano di conservazione dell'archivio	21
12.	IL SISTEMA INFORMATICO	
12.1	La soluzione tecnologica adottata	21
12.2	Descrizione funzionale del Sistema	21
12.3	Descrizione del sistema	
13.	SICUREZZA	
13.1	Obiettivi del piano di sicurezza	22
13.2	Gestione dei documenti informatici – sicurezza	22
13.3	Gestione delle registrazioni di protocollo e sicurezza	22
13.4	Descrizione del sistema	23
13.5	Documento misure minime di sicurezza ICT	23
14.	NORME FINALI E TRANSITORIE	
14.1	Approvazione ed entrata in vigore del manuale	23
14.2	Revisione	23
14.3	Pubblicazione	23
14.4	Norme di rinvio	23

ALLEGATI

1. A1-B-C-D-E-F-G-H-I-L-M-N



1. PRINCIPI GENERALI

1.1 Premessa

Il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 recante le "Regole tecniche per il protocollo informatico", all'articolo 3, comma 1, lettera d), prevede l'adozione del "Manuale di gestione del protocollo informatico, dei documenti e dell'archivio" per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii, Codice dell'Amministrazione Digitale.

Il manuale di gestione, redatto secondo quanto previsto dal successivo art. 5, comma 1, del suddetto DPCM, "descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi". In questo ambito è previsto che ogni amministrazione pubblica individua una o più Aree Organizzative Omogenee, all'interno delle quali viene nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000 e ss.mm.ii).

Obiettivo del manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale sulla quale avviare il processo di ammodernamento e di trasparenza dell'attività dell'amministrazione.

Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente documento, pertanto, si rivolge non solo agli operatori di protocollo, ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.

Il manuale è articolato in due parti: nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema, nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

1.2 Ambito di applicazione

Il presente manuale di gestione del protocollo, dei documenti e degli archivi redatto in applicazione della normativa vigente, in particolare il DPR 445/2000 art. 50 – 67; il D.lgs n. 82/2005, artt. 40-44bis; nonché il DPCM 31 ottobre 2013, descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Unione Territoriale Intercomunale del Torre.

1.3 Norme di riferimento e Definizioni

Ai fini del presente manuale si intende per:

- "**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- "**CAD**", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale e ss.mm.ii.;
- "**Regole tecniche**", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico";
- "**Regole tecniche per la conservazione**" il DPCM del 13 novembre 2014 "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";

Unione Territoriale Intercomunale del Torre



- “**GDPR**” Regolamento Europeo 2016/679 – normativa in materia di protezione dati personali;
- “**Amministrazione**” l’Unione Territoriale Intercomunale del Torre costituita ai sensi della L.R. FVG n. 26/2014 e ss.mm.ii.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea quale insieme di funzioni e di strutture che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi del Testo Unico;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RPA** - Responsabile del Procedimento Amministrativo - il dirigente / funzionario che ha la responsabilità dell’esecuzione degli adempimenti amministrativi relativi ad un affare;
- **SdP** – Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **UOP** – Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UO** Aree/Unità Organizzative/Uffici in cui si articola la struttura dell’AOO
- **PEC** – Posta Elettronica Certificata

1.4. Modello organizzativo

Le procedure previste nel presente Manuale disciplinano in particolare attraverso:

- la ricezione da parte delle UOP – Unità Organizzative di registrazione di Protocollo della documentazione in entrata, la successiva assegnazione alle UO competenti;
- la gestione della corrispondenza in uscita dalle UO dell’Ente;
- la classificazione dei documenti sulla base di un titolario di classificazione, volta ad assicurare la gestione ordinata dell’archivio;
- la formazione dei fascicoli, finalizzata ad una corretta ed efficiente gestione degli archivi.

L’amministrazione ha stipulato con la Regione Autonoma Friuli Venezia Giulia un Protocollo d’Intesa volto a garantire per la AOO l’utilizzo di strumenti finalizzati alla produzione, gestione e conservazione dei documenti informatici in attuazione alle disposizioni normative e regolamentari in materia.

È prevista la riproduzione su carta solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti informatici.

Gli eventuali documenti cartacei ricevuti, dopo registrazione e segnatura di protocollo, sono sottoposti al processo di scansione per la loro dematerializzazione.

Il sistema di protocollazione dell’UTI-TORRE viene gestito da un unico applicativo fornito dalla Regione Autonoma FVG nell’ambito del Protocollo d’Intesa – Repertorio voce “Classe documentale – Protocollo”, che permette gestire le operazioni di protocollazione sia in Entrata che in Uscita da parte delle UOP presenti all’interno dell’AOO.

La scelta di un modello decentrato, riguarda prevalentemente la protocollazione in uscita, risiede nell’esigenza di dare autonomia agli uffici, anche in ragione dei numerosi servizi attribuiti alle U.T.I. dalla L.R. n. 26/2014 e ss.mm.ii e la conseguente numerosità degli atti prodotti dal personale dell’UTI-TORRE.

1.5 Aree Organizzative Omogenee

Per la gestione dei documenti l’Amministrazione ha istituito un’unica Area Organizzativa Omogenea (AOO), denominata “UTI-TORRE”, nell’ambito della quale è istituito un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (**allegato A1**).

1.6 Accreditalimento dell’AOO all’IPA

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

Il codice identificativo dell’amministrazione è stato generato e attribuito all’amministrazione: **utidt**.



L'IPA è accessibile, tramite il relativo sito internet <http://www.indicepa.gov.it> , a tutti i soggetti pubblici o privati.

L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità dell'indirizzo di posta elettronica indicato. Con la stessa tempestività, l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.7 Servizio per la gestione informatica del protocollo

Nella AOO è istituito il Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Al suddetto servizio è preposto il Responsabile del Servizio di Protocollo informatico RSP, della gestione dei flussi documentali e degli archivi.

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

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

1.8 Caselle di Posta Elettronica

L'AOO è dotata di una casella PEC - posta elettronica certificata istituzionale - per la corrispondenza, sia in ingresso che in uscita. Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UO) che ad essa fanno riferimento denominata: uti.torre@certgov.fvg.it .

Tale casella è affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura almeno una volta al giorno della corrispondenza ivi pervenuta.

In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione ha assegnato ai propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, una casella di posta elettronica convenzionale (es. nome.cognome@torre.uti.fvg.it) (**allegato B**).

2. CARATTERISTICHE DEL PROTOCOLLO INFORMATICO

2.1 Unicità del protocollo informatico

Nell'ambito dell'Area Organizzativa Omogenea il registro di protocollo è unico ed è gestito dal Servizio di protocollo informatico,

Il registro di protocollo è atto pubblico di fede privilegiata che certifica le informazioni connesse all'elenco dei protocolli registrati nell'arco di uno stesso giorno. Tale registro soggiace alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa in materia.

Il registro viene generato automaticamente dal sistema



La numerazione delle registrazioni di protocollo è unica e rigidamente progressiva. Essa si chiude al 31 dicembre e ricomincia da 0000001 all'inizio di ogni anno solare.

Il numero di protocollo è costituito da almeno sette cifre numeriche, ai sensi dell'articolo 57 del Testo Unico.

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

2.2 Registro giornaliero di protocollo

Il registro giornaliero di protocollo si genera quotidianamente, mediante produzione automatica, dell'elenco dei protocolli e delle informazioni ad essi connesse, registrati nell'arco di un giorno.

Al fine di garantire l'immodificabilità del contenuto, ai sensi dell'art. 7 c. 5 delle Regole tecniche per il protocollo informatico, il registro giornaliero di protocollo generato automaticamente con identificativo classe documentale "REGPROT", viene inviato e conservato a norma dal Servizio di Conservazione dei documenti informatici affidato alla Regione Autonoma Friuli Venezia Giulia, così come risultante da apposita Convenzione.

3. IL DOCUMENTO

3.1 Formazione del documento amministrativo analogico

A norma dell'art. 1, lett. A DPR 445/2000 per documento analogico si intende la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

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

3.2 Formazione del documento amministrativo informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. (art. 20 CAD).

L'Unione Territoriale Intercomunale del Torre, ai sensi dell'art. 40 e 71 del C.A.D., forma gli originali dei propri documenti con mezzi informatici (utilizzo di strumenti software, acquisizione a mezzo scanner, ecc)

Qualsiasi documento deve riportare un solo protocollo e può fare riferimento a più fascicoli.

La sottoscrizione con firma digitale necessaria alla redazione e perfezione giuridica del documento in uscita devono essere apposte prima della sua protocollazione.

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

Le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- Sottoscrizione con firma digitale
- Trasferimento a soggetti terzi con PEC con ricevuta completa di consegna
- Memorizzazione sui sistemi di protocollo e gestione documentale che adottino politiche di sicurezza
- Apposizione di una validazione temporale (a cura della Regione Autonoma Friuli Venezia Giulia)
- Versamento ad un sistema di conservazione a norma

Al documento informatico immodificabile ed ai documenti soggetti a registrazione particolare vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo è costituito da:

- Identificativo univoco e persistente
- Riferimento temporale
- Oggetto
- Soggetto che ha formato il documento



- Destinatario
- Impronta del documento informatico

Nel caso specifico del documento amministrativo informatico l'insieme dei metadati minimi è costituito da:

- Numero di protocollo
- Data di protocollo
- Mittente – destinatario
- Oggetto
- Data e protocollo del documento ricevuto, se disponibili
- Impronta del documento informatico
- Metadati aggiuntivi stabiliti a fini amministrativi, gestionali e conservativi.

3.4 Documento in arrivo

I documenti in ingresso sono tutti gli atti aventi rilevanza giuridico probatoria prodotti da soggetti esterni ed acquisiti dall'Unione Territoriale Intercomunale del Torre nell'esercizio delle sue funzioni.

I documenti informatici sono recapitati a mezzo posta elettronica convenzionale o certificata, per telefax su supporto rimovibile quale, ad esempio, CD ROM, DVD, tape, pen drive, etc, consegnato direttamente all' UOP o inviato per posta convenzionale o corriere.

I documenti analogici trasmessi da soggetti esterni all'amministrazione sono recapitati a mezzo posta convenzionale o corriere, a mezzo posta raccomandata, telegramma, con consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata all'UOP.

3.5 Documento in partenza

I documenti in uscita sono tutti gli atti aventi rilevanza giuridico probatoria prodotti dal personale dall'Unione Territoriale Intercomunale del Torre nell'esercizio delle proprie funzioni e trasmessi a soggetti esterni.

I documenti informatici sono trasmessi ai destinatari per mezzo della posta certificata PEC. In altri casi, il documento informatico può essere riversato su supporto rimovibile non modificabile ed inviato al destinatario. I documenti su supporto cartaceo sono inviati: a mezzo posta convenzionale, posta raccomandata o corriere oppure a mezzo consegna diretta al destinatario.

3.6 Documento interno

I documenti interni sono tutti gli atti prodotti all'interno dell'Amministrazione, generalmente con tecnologie informatiche e possono essere:

- di natura prevalentemente informativa,
- di natura prevalentemente giuridico-probatoria

I documenti interni di natura informativa quali: mere comunicazioni interne scambiate tra uffici, richieste di materiale di cancelleria, richieste per malfunzionamenti pc non vanno protocollati.

Di regola, lo scambio di tali documenti avviene per mezzo della posta elettronica.

I documenti interni di natura prevalentemente giuridico-probatorio, ossia tutti gli atti redatti dal personale dell'Unione Territoriale Intercomunale del Torre nell'esercizio dell'espletamento delle proprie funzioni, volti a documentare attività istruttorie di competenza, devono essere protocollati.

4. DESCRIZIONE DELLA LAVORAZIONE DEL FLUSSO DOCUMENTALE in ARRIVO

4.1 Ricezione dei documenti informatici

Di norma la ricezione dei documenti informatici è assicurata tramite la casella PEC - posta elettronica certificata istituzionale uti.torre@certgov.fvg.it, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA), accessibile, in ingresso, solo al Servizio del Protocollo Informatico - SdP.

Il personale dell'UOP controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e, previa verifica della bontà e dell'integrità del messaggio, procede alla registrazione di protocollo.



Nel caso in cui il messaggio pervenuto sia illeggibile o incompleto, l'UOP deve segnalare la circostanza al mittente, indicando che lo stesso non verrà sottoposto a protocollazione.

I documenti informatici in arrivo possono essere dotati di firma digitale, di firma elettronica o non firmati.

In particolare, la firma digitale utilizzata per inviare e ricevere documenti da e per l'Amministrazione e per sottoscrivere documenti o qualsiasi altro file digitale con valenza giuridico-probatoria costituisce l'unico strumento che soddisfa i requisiti di sicurezza dell'identificabilità del sottoscrittore, nonché dell'integrità ed immodificabilità del documento. In particolare, a norma dell'art. 1 c.1, lett. N) del Testo Unico, e dell'art. 1, comma 1, lettera S) del CAD, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata consente al firmatario - 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. Inoltre, la certificazione di una chiave pubblica (art. 27 CAD) da parte di una autorità di certificazione garantisce la corrispondenza della chiave con il soggetto che la espone.

Ai sensi dell'art. 21 CAD il documento informatico dotato di firma digitale - avente un certificato valido - si deve reputare equivalente ad un documento cartaceo dotato di firma autografa, in quanto a mente dell'art. 2702 c.c. fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi lo ha sottoscritto.

Il documento dotato di firma elettronica, o "firma digitale debole", soddisfa il requisito della forma scritta e " sul piano probatorio è liberamente valutabile in giudizio" (art. 21, CAD). La firma elettronica assicura solo la provenienza del documento e non l'integrità del contenuto e pertanto la valenza giuridico-probatoria di un messaggio così ricevuto sarà valutabile dal responsabile del procedimento amministrativo.

Qualora il messaggio di posta elettronica non provenga da una casella PEC, ovvero non sia munito di firma digitale, viene comunque protocollato, smistato, ed assegnato. Il Responsabile del procedimento valuta discrezionalmente l'opportunità di utilizzare o meno il documento così pervenuto.

4.2 Ricezione dei documenti cartacei a mezzo posta convenzionale

I documenti analogici che pervengono quotidianamente a mezzo posta sono sottoposti dal personale addetto ad una preliminare verifica in merito all'indirizzo ed al destinatario sugli stessi apposti.

I documenti ricevuti via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, sono trattati come un documento cartaceo.

La busta si allega al documento per la parte relativa ai timbri postali.

Dopo aver accuratamente separato i documenti esclusi dalla registrazione del protocollo di cui all'art. 53, comma 5, del Testo Unico (gazzette ufficiali, bollettini ufficiali e notiziari della pubblica amministrazione note di ricezione delle circolari e altre disposizioni, materiali statistici, atti preparatori interni, giornali, riviste, le newsletter, libri, materiali pubblicitari, inviti) il personale dell'UOP sollecitamente provvede alla registrazione, segnatura, e classificazione dei documenti.

I documenti vengono scannerizzati, con acquisizione del relativo file nel sistema, ed assegnati alla UO di competenza, individuata con atto dell'Ufficio di Presidenza.

4.3 Ricezione di documenti cartacei a mezzo telefax

Al documento ricevuto mediante telefax da parte dei cittadini di norma, non deve far seguito la trasmissione dell'originale in quanto rispetta il requisito della forma scritta.

Nel caso in cui, pervenga in un momento successivo l'originale su quest'ultimo viene apposta la seguente dicitura; "già pervenuto via fax il giorno...".

4.4 Fatture elettroniche, assegni e altri valori di debito o credito

Le fatture elettroniche vengono gestite attraverso il sistema di interscambio messo a disposizione della Regione Autonoma Friuli Venezia Giulia – SDI-FVG, quale intermediario per i servizi connessi alla fattura elettronica per tutti gli enti del territorio e che collocherà direttamente con il *Sistema di Interscambio dell'Agenzia delle Entrate (SDI)*.



Gli assegni o altri valori di debito o credito pervenuti in forma cartacea (v. punto 4.2), vengono protocollati nel sistema SdP ed assegnati all'UO competente.

4.5 Protocollo di documenti inerenti gare di appalto confezionate su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede ad inoltrarla alla UO competente; quest'ultima provvede a sottoscrivere il plico, a riportare sul medesimo la data, l'ora di arrivo ed a riconsegnarla alla UOP per la protocollazione del plico in parola.

Il plico così protocollato viene riconsegnato alla UO che provvede alla custodia, con mezzi idonei, sino all'espletamento della gara.

Dopo l'apertura delle buste, l'UO che gestisce la gara riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

Per motivi organizzativi tutti gli UO sono tenuti ad informare con congruo anticipo il RPA dell'AOO in merito alle scadenze di concorsi, gare, bandi di ogni genere.

4.6 Protocolli urgenti

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

Solo in questo caso il RPA si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale, o cartaceo, da spedire. Tale procedura viene osservata sia per i documenti in ingresso che per quelli in uscita.

4.7 Documenti non firmati - anonimi

L'operatore di protocollo, conformandosi alle regole stabilite dal RSP attesta la data, la forma e la provenienza per ogni documento.

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

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

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

4.8 Messaggi di posta elettronica pervenuti nelle caselle e-mail dei singoli dipendenti

Considerato che l'attuale sistema di posta elettronica convenzionale non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata come segue:

- caso di invio, come allegato, di un documento scansionato munito di firma autografa: fermo restando che il RPA deve verificare la provenienza certa dal documento, in caso di mittente non verificabile, il RPA valuta, caso per caso l'opportunità di trattare il documento, in caso positivo il messaggio verrà reinoltrato dal mittente nella casella PEC dell'Ente per la corretta protocollazione;
- caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale; il RPA dovrà comunicare al mittente di rinviare il messaggio nella casella PEC dell'Ente, al fine della corretta protocollazione;
- caso di invio di una *e-mail* contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

4.9 Integrazioni documentarie

Il UOP non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed gli eventuali allegati.

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



I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale con esplicito riferimento alla registrazione di protocollo “PRECEDENTE”, al fine della corretta gestione del fascicolo.

4.10 Documenti indirizzati nominalmente al personale dell’Unione Territoriale Intercomunale del Torre.

La posta indirizzata nominalmente al personale dell’Unione Territoriale Intercomunale del Torre, è regolarmente aperta e registrata al protocollo, a meno che sulla busta non sia riportata la dicitura “personale” - “riservata personale” o espressione equivalente.

4.11 Protocollazione di un numero consistente di documenti cartacei

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

4.12 Interoperabilità dei sistemi di protocollo informatico

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

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l’utilizzo della posta elettronica è regolata dal Codice dell’Amministrazione Digitale.

4.13 Registrazione e segnatura di protocollo dei documenti ricevuti

Su ogni documento ricevuto dall’Unione Territoriale Intercomunale del Torre è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori. Tale registrazione è eseguita in un’unica operazione, senza possibilità per l’operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene ai sensi dell’art. 53 del Testo Unico, i seguenti dati obbligatori:

- a) il numero di protocollo, generato automaticamente dal sistema;
- b) la data di registrazione di protocollo, assegnata automaticamente dal sistema;
- c) il mittente per i documenti ricevuti o l’Ufficio interno che ha prodotto il documento;
- d) l’oggetto del documento;
- e) la data e il numero di protocollo del documento ricevuto, se disponibili;
- f) luogo di provenienza;
- g) mezzo di ricezione;
- h) tipo documento;
- i) classificazione;
- j) fascicolo (se attiva la funzione);
- k) l’impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

L’operazione di segnatura di protocollo è effettuata contemporaneamente all’operazione di registrazione di protocollo e avviene attraverso il SdP, su report del documento generato automaticamente vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

- codice identificativo riferito al Protocollo Generale dell’U.T.I. del Torre (es. Prot. GEN-GEN)
- data e numero di protocollo del documento (es. 2018-1100P Data gg/mm/aa)

L’operazione di segnatura dei documenti ricevuti in formato cartaceo viene effettuata dall’UOP, attraverso l’apposizione di apposito timbro riportante l’indicazione dell’ente, la data ed il numero di



protocollo assegnato dal sistema, successivamente il documento cartaceo viene acquisito attraverso scansione del documento ed allegato nel SdP.

La segnatura di protocollo deve essere effettuata sulla prima pagina del documento.

I documenti pervenuti alla casella PEC, una volta registrati, sono sottoposti a segnatura automaticamente dal sistema di protocollo informatico.

L'UOP provvede, contestualmente alla segnatura dei documenti ricevuti, a classificare il documento così come riportato nel Titolare.

Nel caso di ricezione di documenti afferenti questioni già in trattazione da parte dell'Amministrazione, il personale dell'UOP, nell'ottica della collaborazione tra Uffici e dell'ottimizzazione dei procedimenti, prima di procedere all'operazione di registrazione ha cura di evidenziare i legami esistenti tra i documenti sulla base delle informazioni reperibili dai documenti stessi o dal sistema di protocollazione mediante l'utilizzo della specifica funzione "PRECEDENTI". In particolare, nel predetto campo (allacci) saranno visionabili tutti gli atti facenti parte di uno stesso procedimento.

4.14 Livello di riservatezza

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

Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale.

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

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

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

4.15 Errata ricezione dei documenti analogici

Qualora all'UOP pervengano erroneamente documenti indirizzati ad altri Enti le buste o i contenitori vanno restituiti. Nel caso in cui la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

4.16 Errata ricezione dei documenti digitali

Nel caso in cui pervengano sulla casella PEC dell'Amministrazione, o in una casella non istituzionale messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa AOO".

4.17 Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici mediante la casella PEC, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell'AOO.

4.18 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Il personale addetto al protocollo non può rilasciare ricevute per i documenti che non sono soggetti a protocollazione. L'apposizione del timbro Unione Territoriale Intercomunale del Torre con la data e l'ora d'arrivo e la sigla dell'operatore sulla copia non ha alcun valore giuridico.

Quando il documento cartaceo non soggetto a protocollazione è consegnato direttamente ad una UOP ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a fotocopiare gratuitamente la prima pagina del documento e apporvi il timbro dell'Unione Territoriale Intercomunale del Torre con la data e l'ora d'arrivo e la sigla dell'operatore incaricato.



Nel caso, invece, si tratti di documenti soggetti a protocollazione, quando il documento cartaceo è consegnato direttamente ad una UOP ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve deve rilasciare la ricevuta in questione o può fotocopiare gratuitamente la pagina del documento su cui è stata apposta la segnatura di protocollo.

4.19 Elementi facoltativi delle registrazioni di protocollo

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

La registrazione degli elementi facoltativi del protocollo, può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UO.

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

4.20 Termini per la registrazione di protocollo

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre due giorni lavorativi dal ricevimento, nel caso di oggettive impossibilità alla registrazione.

4.21 Differimento dei termini di registrazione

Nel caso di eccezionale carico di lavoro, che non permette di evadere la corrispondenza ricevuta nei tempi sopra indicati e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa risultare lesa un diritto di terzi (es. partecipazione concorso), con motivato provvedimento del dirigente dell'UOP è autorizzato l'uso del *protocollo differito*.

In particolare, il *protocollo differito* consiste nell'adozione di un provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata. Si applica solo ai documenti in arrivo e per tipologie omogenee che il dirigente dell'UOP deve descrivere nel provvedimento.

4.22 Annullamento delle registrazioni di protocollo

I dati obbligatori relativi alla registrazione di protocollo non sono modificabili. La necessità di eventuali modifiche, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Solo il RsP Responsabile del Servizio per la tenuta del protocollo, è autorizzato ad annullare, ovvero a dare disposizioni al RPA di annullare le registrazioni di protocollo. L'annullamento di una registrazione di protocollo generale deve essere richiesto dall'UO con specifica comunicazione, inviata al RsP, adeguatamente motivata.

Ai sensi degli artt. 54 e 61 del "Testo Unico", i dati annullati e/o modificati rimangono memorizzati nella procedura del protocollo informatico unitamente alle informazioni relative all'ora, alla data, al nominativo dell'operatore che effettua l'operazione.

5. REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI

5.1 Regole generali

Generalmente, con l'assegnazione si procede all'individuazione dell'UO competente e destinatario del documento, e quindi al conferimento della responsabilità del procedimento amministrativo, mentre l'attività di smistamento consiste nell'inviare il documento protocollato e segnato all'UO medesimo.

L'assegnazione può essere effettuata per conoscenza o per competenza, e può essere estesa a tutti i soggetti ritenuti interessati, al fine di consentire la massima condivisione delle informazioni.

All'atto dell'assegnazione il Responsabile dell'UO di competenza - che provvede alla presa in carico del documento ed, in applicazione delle disposizioni organizzative in atto, all'eventuale sub-assegnazione al responsabile dell'istruttoria - verifica la corretta classificazione del documento (eventualmente correggendola), inserisce il documento in apposito fascicolo elettronico e provvede alla lavorazione o all'archiviazione del documento.



I termini per la definizione del procedimento amministrativo che prende avvio da un determinato documento (esposto, segnalazione, richiesta parere...), decorrono comunque dalla data di protocollazione.

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

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

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

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

5.2 Regole disponibili con il SdP

L'assegnazione dei documenti protocollati e segnati avviene sfruttando le funzionalità del SdP.

Il SdP, per abbreviare il processo di assegnazione del materiale documentario oggetto di lavorazione, utilizza l'organigramma dell'AOO.

All'assegnazione segue la presa in carico del documento da parte del RPA, che provvede a inoltrarlo, se del caso, all'addetto istruttore della pratica. In questa sede viene eseguita la classificazione del documento secondo le voci del titolario (**Allegato C**).

5.3 Attività di assegnazione

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

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

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

Il SdP memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante anche ai fini di individuare i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

5.4 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UO competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile.

L'UO competente ha notizia dell'assegnazione di detti documenti tramite un messaggio generato automaticamente dal sistema, quale notifica di assegnazione.

Il responsabile dell'UO è in grado di visualizzare i documenti, attraverso le funzionalità del SdP e, in base alle abilitazioni possedute, potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente per la materia a cui si riferisce il documento ed assegnare il documento in questione.

La "presa in carico" dei documenti informatici viene registrata dal SdP in modo automatico e la data di ingresso dei documenti negli UO competenti coincide con la data di assegnazione degli stessi.

I destinatari del documento per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale.

5.5 Assegnazione dei documenti ricevuti in formato cartaceo



Al termine delle operazioni di registrazione, segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione. L'originale cartaceo riceve il seguente trattamento:

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

I documenti cartacei gestiti dalla UOP sono di norma assegnati entro il giorno successivo a quello di ricezione, salvo che vi figurino, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

L'UO competente ha notizia dell'arrivo del documento ad esso indirizzato tramite un messaggio di posta elettronica. Attraverso le funzioni del SdP e in base alle abilitazioni previste il responsabile dell'UO potrà:

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

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

5.8 Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UO che riceve il documento comunica l'errore alla UOP, che procederà ad una nuova assegnazione.

Nel caso in cui un documento assegnato erroneamente ad un UO afferisca a competenze attribuite ad altra UO, l'abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UO medesima, o a persona da questi incaricata.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

6. GESTIONE DELLA CORRISPONDENZA IN PARTENZA

6.1 Trasmissione dei documenti

Per documenti in partenza s'intendono quelli prodotti dagli uffici dell'Unione Territoriale Intercomunale del Torre, nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria e destinati a essere trasmessi a soggetti terzi o ad altre amministrazioni.

Ai fini di una maggiore efficienza gestionale l'Unione Territoriale Intercomunale del Torre utilizza le tecnologie quali PEC e firma elettronica e digitale.

Per la spedizione dei documenti informatici, l'Unione Territoriale Intercomunale del Torre si avvale della casella PEC posta elettronica certificata istituzionale (uti.torre@certgov.fvg.it).

I documenti in partenza verso destinatari esterni all'Amministrazione. sono classificati secondo il Titolario di classificazione (**allegato C**), firmati digitalmente ed allegati alla registrazione di protocollo, attraverso la funzionalità del sistema GIFRA (**Allegato I**) dal personale dell'UOP addetto alla protocollazione in partenza, che ha altresì la responsabilità:

- del loro inserimento nel fascicolo relativo al procedimento
- della loro archiviazione.

In particolare, al momento della protocollazione degli atti in uscita vanno inserite nel sistema tutte quelle informazioni (PRECEDENTI e/o annotazioni. etc.) ritenute necessarie per favorire una agevole ricerca degli atti, nonché un eventuale successivo monitoraggio delle pratiche stesse.

I documenti informatici, **sottoscritti con firma digitale** conforme alle disposizioni dettate dalla normativa, basata su un certificatore accreditato e generata con un dispositivo sicuro, sono trasmessi **esclusivamente** attraverso la PEC. Solo la trasmissione dalla casella PEC istituzionale ad una casella PEC del destinatario costituisce evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art.47 CAD).

Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui al GDPR Regolamento Europeo 2016/679 e del decreto legislativo 30/06/2003, n. 196, l' art. 46 del CAD dispone che "i documenti



informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.”

Le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono eventualmente conservate all'interno del relativo fascicolo.

Nei casi in cui il destinatario sia sprovvisto di un indirizzo di posta elettronica, il documento potrà essere prodotto in formato analogico, sottoposto a scansione e firmato digitalmente, per poter essere caricato nel Sistema del Protocollo al fine della corretta conservazione a norma. I mezzi di recapito della corrispondenza, in quest'ultimo caso, sono:

1. il servizio di posta ordinaria o posta raccomandata;
2. consegna diretta al destinatario.

Per la posta in PARTENZA viene utilizzato un modello contenente i seguenti dati obbligatori:

- ❖ logo dell'Unione Territoriale Intercomunale del Torre;
- ❖ indicazione dell'Area Organizzativa Omogenea e dell'UO che ha prodotto il documento;
- ❖ indirizzo PEC di posta elettronica certificata;
- ❖ indirizzo completo con numero di telefono e fax;
- ❖ data completa, luogo, giorno, mese, anno;
- ❖ numero degli allegati, se presenti;
- ❖ oggetto del documento;
- ❖ firma elettronica avanzata/qualificata da parte del responsabile del procedimento e/o del responsabile del provvedimento finale;

Il documento informatico correttamente protocollato rispetta le regole riportate al punto 3.2 “documento informatico” del presente Manuale.

Qualora si verifichi un errore di consegna della comunicazione a causa di indirizzo inesistente (es. ‘dominio non trovato’) o momentaneamente non disponibile, l'UO riceve una notifica di errore che viene acquisita e protocollata in ingresso e smistata all'Ufficio Tecnico Informatico di competenza. La comunicazione viene esaminata e viene a sua volta assegnato all'UOP che ha protocollato il documento in uscita, con indicazioni dell'errore e delle modalità per effettuare un nuovo invio dello stesso protocollo in uscita.

Una volta ricevuta comunicazione di avvenuta consegna, l'assegnatario deve mettere agli atti la notifica di mancata consegna ricevuta.

6.2 Spedizione dei documenti su supporto cartaceo

Ad ogni UOP competono le seguenti operazioni:

- ❖ eseguire le operazioni di registrazione di protocollo, segnatura di protocollo;
- ❖ imbustazione, se necessario l'utilizzo del Servizio Postale.

Nel caso di spedizione per raccomandata con ricevuta di ritorno, posta celere, corriere, o altro mezzo che richieda una qualche documentazione da allegare alla busta, questa modulistica viene compilata a cura degli Uffici competenti e successivamente inoltrata agli addetti alla spedizione, al fine della pesatura, calcolo delle spese postali, tenuta della relativa contabilità e spedizione.

Gli uffici devono far pervenire quanto sopra indicato agli addetti alla spedizione entro le ore 11.00, oltre tale termine la posta verrà spedita il giorno successivo.

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

7.1 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo: le gazzette ufficiali, i bollettini ufficiali e notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni.

Sono altresì esclusi dalla registrazione di protocollo i documenti già soggetti a registrazione particolare dell'Amministrazione elencati 7.2.



7.2 Documenti soggetti a registrazione particolare

Le deliberazioni di Assemblea dei Sindaci, dell'Ufficio di Presidenza, i decreti del Presidente, le determinazioni organizzative, i decreti sono documenti già soggetti a registrazione particolare dell'Amministrazione e non vanno registrati al protocollo a condizione che siano implementate funzionalità software che consentano di eseguire su di essi tutte le operazioni previste nell'ambito della gestione dei documenti.

Questi documenti costituiscono delle serie archivistiche, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

- ❖ i dati identificativi di ciascun atto;
- ❖ i dati di classificazione e fascicolazione;
- ❖ il numero di repertorio che è un numero progressivo, annuale.

I contratti vengono registrati nel SdP nella sezione dedicata al **REPERTORIO DEI CONTRATTI**, attraverso la compilazione degli appositi campi, il contratto formato esclusivamente in formato elettronico e con apposizione delle firme digitali, viene caricato nel sistema e conservato a norma.

8. REGISTRO DI EMERGENZA

8.1 Il registro di emergenza

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

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

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

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

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

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

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

8.2 Modalità di apertura del registro di emergenza

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica *realtime*, le operazioni di protocollo siano svolte sul registro di emergenza cartaceo.

Sul registro di emergenza sono riportate: la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale (**allegato D**).

9. ACCESSO AL SISTEMA

9.1 Abilitazione per l'accesso all'uso del sistema SdP - GIFRA

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (*UserID*) e privata (*Password*) ed un sistema di autorizzazione basato sulla profilazione preventiva degli utenti (**allegato E**).

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

Queste, in sintesi, sono:

- *Consultazione* - per visualizzare in modo selettivo le registrazioni di protocollo eseguite da altri;
- *Inserimento* - per inserire gli estremi di protocollo, effettuare una registrazione di protocollo ed associare i documenti;



- *Modifica* - per modificare i dati opzionali di una registrazione di protocollo;

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

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

Il SdP fruito dall'AOO:

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

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

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

9.2 Abilitazioni

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.

Per quanto concerne i documenti sottratti all'accesso, si rinvia allo specifico Regolamento per l'accesso degli atti.

Si fornisce nell'**allegato E)** l'elenco delle abilitazioni all'utilizzo del sistema di gestione informatica dei documenti.

9.3 Utenti esterni alla AOO 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.

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss. del d.lgs 7 marzo 2005 n. 82 e smi.

9.4 Utenti esterni alla AOO - Privati

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

10. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE

10.1 Classificazione dei documenti

Tutti i documenti ricevuti e prodotti dagli uffici dall'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al Titolario riportato nell'**allegato C)**, tale documento è suscettibile di aggiornamento e non è retroattivo, pertanto non si applica ai documenti protocollati prima della sua introduzione.

Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO. Esso consente di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

Al fine di agevolare e normalizzare, da un lato, la classificazione archivistica e, dall'altro, l'assegnazione per competenza, sul SdP è stato predisposto un elenco degli Uffici Utente e dei dipendenti unitamente a quello di classificazione. L'elenco è una guida rapida di riferimento, in ordine alfabetico che, sulla base del Titolario, permette l'immediata individuazione della classificazione e delle competenze.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe), il riferimento al fascicolo.



Le operazioni di classificazione vengono svolte in momenti diversi: l'addetto alla registrazione di protocollo inserisce la voce di livello più alto (titolo), mentre l'attribuzione delle voci di dettaglio (classi) è demandata all'UO di competenza.

10.2 Fascicolazione dei documenti

Ogni documento, dopo la classificazione, viene inserito a cura dell'UO nel fascicolo di riferimento.

Ai sensi dell'art. 52 del Testo Unico il sistema di protocollo informatico fornisce – tra l'altro – anche *“le informazioni sul collegamento esistente tra ciascun documento ricevuto e i documenti dalla stessa formati nell'adozione del provvedimento finale”*.

Pertanto, il fascicolo informatico è lo strumento che consente l'accorpamento dei documenti all'interno del sistema di protocollo informatico in base all'affare o al procedimento, essi sono archiviati all'interno di ciascun fascicolo secondo l'ordine cronologico di registrazione.

La fascicolazione viene gestita attraverso le funzioni ad essa dedicate nel sistema GIFRA.

Le operazioni per l'apertura di un nuovo fascicolo possono avvenire da:

- Ufficio, Registro, Anno e Numero in caso di selezione da “Registro”;
- Classifica, Anno e Numero per pratiche da “Classifica”

Le informazioni minime per l'apertura di un nuovo fascicolo sono il repertorio da utilizzare (da registro o da classifica), l'Anno di riferimento e l'Oggetto.

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

11. CONSULTAZIONE, MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO, STORICO E CONSERVAZIONE

11.1 Principi generali

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

11.2 Consultazione ai fini giuridico-amministrativi

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

1. Il diritto di accesso è escluso:

- a. per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
- b. nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
- c. nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
- d. nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.

Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.



Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:

- quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
- quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
- quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
- quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
- quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale.

11.3 Consultazione da parte di personale interno all'amministrazione

Tutti i documenti dell'AOO sono disponibili attraverso la funzione di "interrogazione", accessibile per competenza dagli utenti assegnati alle UO attraverso autenticazione nell'applicativo Gestione del Sistema del Protocollo Informatico - GIFRA, così come indicato **nell'allegato E)** del Manuale di Gestione.

11.4 Consultazione da parte di personale esterno all'amministrazione

La domanda di accesso ai documenti viene presentata/inviata alla UOP, che provvede a smistarla al'UO che ha formato il fascicolo per competenza.

La consultazione dei documenti è possibile sotto la diretta sorveglianza del personale addetto.

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

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

11.5 Diritto di accesso e tutela dei dati personali

I procedimenti amministrativi unitamente al sistema e-prot sono ispirati al rispetto delle norme in materia di diritto di accesso e di protezione dei dati personali e sensibili di cui al Codice in materia di protezione dei dati personali.

L'Amministrazione disciplina il diritto di accesso e la consultazione per fini amministrativi da parte di terzi dei documenti amministrativi, e dei fascicoli formati o detenuti stabilmente dall'Amministrazione, in conformità alla normativa vigente.

Il Regolamento è pubblicato sul sito web dell'Unione Territoriale Intercomunale del Torre.



L'accesso si esercita mediante apposita istanza motivata, indirizzata all'Ufficio competente, utilizzando i moduli allegati al regolamento.

L'Amministrazione a cui sono riconducibili i dati di protocollo e quelli personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria competenza dà attuazione alle disposizioni di cui all'allegato B del Codice in materia di protezione dei dati personali con atti aventi rilevanza interna ed esterna.

Il personale preposto all'apertura e alla registrazione della corrispondenza deve essere regolarmente autorizzato al trattamento dei dati personali; nell'esercizio delle proprie funzioni è tenuto all'osservanza del segreto d'ufficio, nonché dei doveri e degli obblighi previsti dalla normativa di riferimento, a non trarre benefici personali o a nuocere a terzi e all'immagine dell'Unione Territoriale Intercomunale del Torre, dalla conoscenza di particolari circostanze desumibili dai documenti.

Qualora la corrispondenza riservata personale venga recapitata per errore ad un diverso Ufficio, a tutela dei dati personali e /o sensibili eventualmente contenuti, va restituito integro (non vanno aperte le buste o i contenitori) nella stessa giornata, all'UOP.

11.6 Scambio di documenti all'interno della AOO

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

Gli uffici organizzativi di riferimento (UO) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005 concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

11.7 Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei

Tutti i documenti informatici vengono memorizzati direttamente nel SdP nella fase di protocollazione e conservati a norma così come previsto nel capitolo successivo.

Le rappresentazioni digitali dei documenti su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema del Protocollo Informatico, in modo non modificabile, al termine del processo di scansione.

11.8 Conservazione dei documenti informatici

L'Unione Territoriale Intercomunale del Torre si avvale del "Servizio di conservazione a norma dei documenti informatici" in server-farm, messo a disposizione dalla Regione Autonoma Friuli Venezia Giulia, nell'ambito del Protocollo d'Intesa 2014-2018, secondo quanto previsto dagli artt. 44 e ss. del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale - CAD), e dalle regole tecniche di cui all'articolo 71 del CAD, dalla Deliberazione CNIPA n. 11 del 19 febbraio 2004 e loro successive modificazioni o integrazioni, così come risultante dal Manuale di Conservazione (**allegato N**) approvato con Deliberazione dell'Ufficio di Presidenza n. 7/2016 "Approvazione della Convenzione per l'adesione al SERVIZIO DI CONSERVAZIONE A NORMA DEI DOCUMENTI INFORMATICI ai sensi del D.Lgs. n. 82/2005 e s.m.i. (SIAL 2014-2018) ed autorizzazione alla stipula" reperibile nel sito istituzionale dell'ente alla pagina dedicata: <http://www.torre.utifvg.it/index.php?id=6797>.

L'Amministrazione con Decreto del Presidente n. 12/2016 ha individuato il Responsabile della Conservazione ed il delegato.

La conservazione a norma riguarda i soli documenti che siano correttamente formati secondo le indicazioni fornite con le sopra richiamate regole tecniche e si impegna a fornire all'AOO, tramite la propria società *in house* Insiel s.p.a., indicazioni specifiche scritte a cui attenersi per la formazione corretta di documenti informatici da portare in conservazione.

La Regione Autonoma Friuli Venezia Giulia, nell'ambito del Servizio di conservazione a norma dei documenti informatici:

- assicura la consultabilità, l'inalterabilità e l'integrità nel tempo dei documenti mediante lo sviluppo del processo di conservazione;
- garantisce l'applicazione delle misure di sicurezza di cui agli artt. 31 e ss. del Codice della Privacy



- e del DGRP attraverso il supporto e l'attività svolta dalla propria società *in house* Insiel s.p.a.,
- provvede a far apporre una firma digitale e una marca temporale su ciascun lotto di documenti;
- provvede a fornire assistenza durante le fasi di esibizione dei documenti agli organi preposti;
- provvede a tenere, aggiornare e conservare il Manuale del Servizio di conservazione dei Documenti informatici, assicurandone la disponibilità in sede di esibizione, comunicando all'Amministrazione gli aggiornamenti tecnologici e le migliorie funzionali;
- assicura, per il tramite della propria società *in house* Insiel s.p.a., la gestione degli strumenti hardware, del software di sistema e del software di conservazione necessari per la realizzazione del processo oggetto del presente atto, impiegando metodologie aggiornate che ne assicurino precisione, tempestività e sicurezza;
- procede alla memorizzazione e conservazione dei documenti, come previsto dall'art. 44 del CAD e dagli articoli 3 e 5 della Deliberazione CNIPA n. 11/2004, e loro successive modificazioni o integrazioni.

11.9 Piano di conservazione dell'archivio

Il piano di conservazione dell'archivio dell'AOO, è stato redatto conformemente al Titolare di classificazione ed al Manuale di Conservazione di cui al punto 11.3 (**allegato F**).

Il suo aggiornamento compete esclusivamente al responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ed è assicurato quando se ne presenta la necessità, nel pieno rispetto delle disposizioni contenute nella normativa vigente in materia di formazione e conservazione degli archivi, anche in funzione dell'attivazione di nuovi servizi di cui alla L.R. 26/2014 e ss.mm.ii..

Dopo ogni modifica del Titolare, il suddetto responsabile provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche

12. SISTEMA INFORMATICO

12.1 La soluzione tecnologica adottata

Realizzato dalla ditta INSIEL di Trieste e certificato dall'Archivistica Nazionale il programma per la gestione del protocollo Informatico è stato sviluppato mediante il linguaggio di programmazione Power Builder utilizzando quale base dati, di data base relazionale Oracle.

La struttura della base dati e' organizzata secondo l'architettura client/server che consente di distribuire tra macchine in rete il database propriamente detto (lato Server) e i programmi applicativi (lato Client).

Sul Server risiede dunque il database, ove questa denominazione sta ad indicare in Oracle il complesso di oggetti fisici, memoria e processi atti alla gestione dei dati.

In conclusione la soluzione tecnologica adottata fornisce al sistema applicazioni client/server in ambiente visuale sotto Windows 95-98-NT-2000-Xp, a 32 bit native (accesso diretto al database relazionale in rete locale e remota) con linguaggio SQL: infatti nell'applicazione Client/server, i comandi SQL (istruzioni) presenti nei programmi client vengono eseguiti dal motore relazionale server e i risultati vengono restituiti al client: nell'architettura dell'Ente i Personal Computer client lavorano in ambiente Windows mentre il server opera in ambiente Unix.

12.2 Descrizione funzionale del Sistema.

Dal punto di vista funzionale ogni client dispone di due macrofunzioni denominate :

- gestione Protocollo (icona contrassegnata da un notes di colore verde) Viene utilizzata per registrare i dati secondo le disposizioni del T.U.
- gestione Sistema (icona contrassegnata da un raccoglitore di colore grigio) In cui sono presenti le funzioni di interrogazione, stampa, codifica e abilitazione accessi.

La chiave di accesso, determina le modalità mediante le quali l'utente accede al sistema ovvero ogni codice utente può essere personalizzato per permettere un' accesso differenziato alle varie funzioni.



Ogni altra informazione di dettaglio relativa alla descrizione funzionale del sistema può essere rilevata consultando i tre manuali presenti in allegato ovvero :

SAR-31-U0-MOU/996003 Manuale operativo del Supervisore del Sistema (allegato **G**)

SAR-31-U0-MOU/996001 Manuale operativo per la Gestione del Sistema (allegato **H**)

SAR-31-U1-MOU/996001 Manuale operativo per la Protocollazione (allegato **I**)

Infine per certificare l'applicazione ai sensi del testo unico precedentemente citato, si fornisce in allegato il documento Insiel :

Compatibilità applicazione "PROTOCOLLO" e DPR 445/2000 (allegato **L**).

13. SICUREZZA

13.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

13.2 Gestione dei documenti informatici - sicurezza

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

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

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;

- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

13.3 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul SdP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali, che abbiano ad oggetto le operazioni effettuate sul SdP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log dei dispositivi di protezione periferica del sistema informatico (*intrusion detection system-IDS, sensori di rete e firewall*),
- dalle registrazioni dell'applicativo SdP;

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:



- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione;

13.4 Descrizione del sistema

Al fine di indicare le misure di sicurezza, in seguito esposte, si evidenzia che il programma di gestione documentale viene fornito dalla Regione Autonoma Friuli Venezia Giulia, nell'ambito del Protocollo d'Intesa sottoscritto con l'Unione Territoriale Intercomunale del Torre, per la prestazione di servizi forniti nell'ambito del Sistema Informativo Integrato Regionale S.I.I.R.

I dati sono conservati in Server Farm dalla Regione Autonoma Friuli Venezia Giulia, così come stabilito nella convenzione CRM SIAL sottoscritta con la Regione.

Software Applicativo

Gestione Protocollo Web della ditta Insiel S.p.A. di Trieste

Salvataggio dei dati e Garanzie di Conservazione

A cura della Regione Autonoma Friuli Venezia Giulia a seguito sottoscrizione di apposito disciplinare per la conservazione a norma dei documenti informatici per l'U.T.I del Torre.

13.5 Documento Misure Minime di sicurezza ICT

L'Amministrazione ha predisposto ed inoltrato all'AGENZIA PER L'ITALIA DIGITALE - AGID - PRESIDENZA DEL CONSIGLIO DEI MINISTRI il Documento Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni, in data 31/12/2017 (**allegato M**).

14. NORME FINALI E TRANSITORIE

14.1 Approvazione ed entrata in vigore del manuale

Il presente manuale viene adottato dall'Assemblea dei Sindaci dell'Unione Territoriale Intercomunale del Torre, su proposta del Responsabile per la tenuta del protocollo ed entra in vigore dopo la sua approvazione e pubblicazione nei termini di legge.

14.2 Revisione

Il presente manuale viene rivisto ogni volta che si presenta la necessità.

14.3 Pubblicazione

Il manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet dell'amministrazione www.torre.utifvg.it, l'affissione all'Albo Pretorio on-line e l'invio di copia alla Soprintendenza Archivistica per la Regione Autonoma Friuli Venezia Giulia.

14.4 Norme di rinvio

Per tutto quanto non previsto dal presente regolamento valgono le disposizioni di legge previste in materia.