COMUNE DI MASSA

Medaglia d'Oro al Merito Civile

Comune di Massa

Manuale di Gestione del Protocollo Informatico, dei Flussi Documentali e degli Archivi

Approvato con delibera della Giunta Comunale n. 365 del 28/11/2019.

Sommario

I - PRINCIPI GENERALI

Art. 1 - Oggetto

Il presente Manuale di Gestione, adottato ai sensi della normativa vigente (artt. 3 e 5 del DPCM 3/12/2013 *Regole tecniche per il protocollo informatico*), descrive e disciplina le attività di formazione, registrazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici del **Comune di Massa.** L'Amministrazione ha adottato un sistema di gestione documentale avanzato di protocollazione informatica sicuro, certificato e con piena validità giuridica, che consente di avviare progressivamente processi di dematerializzazione della documentazione. Il manuale di gestione fornisce le indicazioni per realizzare i processi di innovazione, che porteranno ad attuare, tramite le nuove tecnologie, la gestione documentale in modalità esclusivamente informatica. Al fine di garantire lo sviluppo del processo di digitalizzazione previsto dalla normativa vigente l'Ente provvede a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese

Art. 2 - Definizioni

Ai fini del presente manuale di gestione si intende per:

- "**AMMINISTRAZIONE**", il Comune di Massa;
- "**TESTO UNICO**", il D.P.R. 20.12.2000, n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- "**REGOLE TECNICHE**", il D.P.C.M. 3.12.2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del Codice dell'Amministrazione Digitale";
- "**C.A.D.**", il D. Lgs. 7.3.2005, n. 82 recante "Codice dell'amministrazione digitale";
- "**AOO**", l'Area Organizzativa Omogenea;
- "**MdG**", il Manuale di Gestione;
- "**DOCUMENTO AMMINISTRATIVO**", ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;
- "**DOCUMENTO INFORMATICO**", la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- "**PROTOCOLLO**", l'insieme delle procedure e degli elementi attraverso i quali i documenti vengono trattati sotto il profilo giuridico-gestionale;
- "**SEGNATURA DI PROTOCOLLO**", l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso;
- "**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 comunale, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati;
- "**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 comunale per la gestione dei documenti;
- "**TODOLIST**", la scrivania virtuale associata ogni utente dell'ente. E' un luogo "informatico" dove i documenti stazionano. Nell'ambito del sistema di gestione informatica dei documenti ToDoList è, quindi, un "punto" della struttura avente la capacità di movimentare o visionare dei documenti. La ToDoList, relativa al Protocollo Informatico, è suddivisa in sezioni, ogni sezione corrisponde nella realtà ad una pila di

documenti o ad un cassetto:

- Arrivo - Presa in Carico : la pila dei documenti ricevuti/assegnati, una sorta di buca della posta in arrivo relativamente alla quale non è ancora stata fatta un'azione di presa in carico.

  Normalmente questa pila rappresenta il lavoro corrente dell'ufficio o persona/e, a cui la scrivania è associata;
- Collegamento alla Pratica : la pila dei documenti già arrivati e di cui è stata fatta un'azione di presa in carico. Normalmente questa pila rappresenta il lavoro corrente dell'ufficio o persona, a cui la scrivania è associata e che deve essere inserito in una o più pratiche;

- "**FASCICOLO**", l'unità archivistica che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare;
- "**CLASSIFICAZIONE**", l'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;
- "**FASCICOLAZIONE**", l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;
- "**ARCHIVIO**", il complesso dei documenti prodotti e acquisiti nello svolgimento della propria attività e l'esercizio delle proprie funzioni dall'amministrazione comunale. Fanno parte dell'archivio del Comune di Massa anche gli archivi e i documenti acquisiti per dono, deposito, acquisto o qualsiasi altro titolo. L'archivio è suddiviso funzionalmente in:
  - ARCHIVIO CORRENTE: il complesso dei documenti relativi a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente;
  - ARCHIVIO DI DEPOSITO: il complesso dei documenti relativi a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico;
  - ARCHIVIO STORICO: il complesso dei documenti relativi a procedimenti conclusi da oltre 40 anni e destinati, previa operazione di scarto, alla conservazione perenne nella sezione separata d'archivio;
- "**FIRMA ELETTRONICA QUALIFICATA**", un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lett. r) del d. lgs.7 marzo 2005, n. 82);
- "**FIRMA DIGITALE**", un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare 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 (art. 1 comma 1 lett. s) del d. lgs.7 marzo 2005, n. 82);
- "**POSTA ELETTRONICA CERTIFICATA (PEC)**", un sistema di comunicazione simile alla posta elettronica tradizionale a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da rendere i messaggi opponibili a terzi;
- "**INTERPRO**", il sistema di protocollo interoperabile della Regione Toscana. Il sistema consente a due sistemi di protocollo informatico di amministrazioni della Regione Toscana di scambiarsi documenti informatici con trattamento automatico;
- "**CONSERVAZIONE A NORMA**", il processo di conservazione dei documenti informatici ai sensi della deliberazione CNIPA 19 febbraio 2004, n.11 e dalle "Regole tecniche" DPCM 13/12/2013;
- "**SUPPORTO DI MEMORIZZAZIONE**", il mezzo fisico che consente la memorizzazione di documenti digitali mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD) oppure mediante l'impiego della tecnologia "flash" (quale ad esempio chiavette removibili usb).

Art. 3 - Area Organizzativa Omogenea (AOO)

Per la gestione unica e coordinata dei documenti, l'Amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata Comune di Massa, come meglio specificato nella scheda riportata nell'Allegato "A" del presente MdG.

Art. 4 - Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

Ai sensi della normativa vigente (TESTO UNICO e REGOLE TECNICHE), l'Amministrazione istituisce il "Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi", individuandolo nell'Ufficio a cui afferiscono le funzioni del protocollo come da Funzionigramma (Allegato B) approvato con delibera di GM n. 45/2019.

Il Servizio svolge i seguenti compiti:

a. garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
b. garantisce la produzione e conservazione del registro giornaliero di protocollo;
c. cura che le funzionalità del sistema, in caso di guasti o anomalie, vengano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
d. garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;
e. effettua le operazioni di annullamento delle registrazioni di protocollo;
f. vigila sull'osservanza delle disposizioni del presente MdG da parte del personale autorizzato e degli incaricati;
g. cura, ai sensi della normativa vigente, il trasferimento dei documenti dagli uffici all'archivio di deposito e la conservazione dell'archivio stesso;
h. cura il costante aggiornamento del presente MdG e di tutti i suoi allegati.

Art. 5 - Il registro informatico di protocollo

1. Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici. E' unico per tutto l'ente, si apre il 1° gennaio e si chiude il 31 dicembre di ogni anno.
2. Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
3. Ai sensi della normativa vigente, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine di ogni giornata lavorativa, è firmato digitalmente dal Responsabile del "Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi" e inviato al sistema di conservazione.
4. La competenza della conservazione del registro è a carico del Responsabile della Conservazione (Regole Tecniche in materia di conservazione – DPCM 3/12/2013).

Art. 6 - La casella di posta elettronica certificata istituzionale

1. L'AOO è dotata di una casella di Posta Elettronica Certificata (PEC) istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA) a costituirne l'unico domicilio digitale;
2. La casella PEC istituzionale del Comune di Massa è **comune.massa@postacert.toscana.it**
3. La casella PEC istituzionale è collegata al sistema di protocollo informatico ed è presidiata, attraverso specifiche funzioni :
    a. per la ricezione di documenti, solo dall'Ufficio Protocollo

b. per la spedizione di documenti all'esterno da qualunque ufficio.

Art. 7 - Il protocollo informatico

Tutti i documenti inviati e ricevuti dall'Amministrazione sono registrati all'interno del registro di protocollo informatico; pertanto, con l'entrata in funzione del sistema di gestione informatica del protocollo, tutti i registri particolari e di settore sono aboliti ed eliminati.

Art. 8 - Interoperabilità del sistema di protocollo informatico.

1. L'interoperabilità di protocollo permette a due sistemi di protocollo informatico di trattare in maniera automatica l'uno le informazioni trasmesse dall'altro. Il sistema consente quindi lo scambio di documenti digitali tra amministrazioni e ne permette il trattamento automatico al protocollo.
2. Il sistema software di protocollo informatico e gestione documentale in uso al Comune di Massa è conforme alla piattaforma tecnologica InterPRO di Regione Toscana e consente l'interscambio dei documenti di protocollo e le relative informazioni accessorie con sistemi di altri Enti Toscani.
3. Il sistema di protocollo interoperabile InterPRO , attraverso specifiche funzioni, è presidiato :
    a. per la ricezione di documenti, solo dall'Ufficio Protocollo
    b. per la spedizione di documenti all'esterno da qualunque ufficio.

II - RESPONSABILITA'

Art. 9 - Responsabile della gestione documentale

1. Il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi provvede a:
    a. individuare gli utenti dell'amministrazione che utilizzano il sistema di protocollo informatico ed attribuire loro un livello di autorizzazione all'uso di funzioni della procedura informatica come meglio specificato nel successivi articoli 10,11,12,13,14;
    b. verificare che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro 24 ore dal fermo delle attività di protocollazione informatica;
    c. controllare il buon funzionamento degli strumenti e dell'organizzazione delle attività di protocollazione
    d. autorizzare le operazioni di annullamento e modifica delle registrazioni di protocollo;
    e. controllare l'osservanza delle presenti norme da parte del personale addetto;
    f. promuovere la formazione e l'aggiornamento degli operatori;
    g. promuovere, periodicamente, opportune verifiche sulle tipologie di documenti protocollati.
2. Il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi svolge un ruolo di coordinamento e d'indirizzo nei confronti delle strutture dell'Ente, al fine di garantire l'uniformità dell'attività di protocollazione.
3. Il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi svolge le funzioni relative alla tenuta e alla gestione del protocollo informatico, esso inoltre:
    a. costituisce il punto centralizzato di spedizione della corrispondenza in partenza dall'Amministrazione;
    b. cura il ritiro della corrispondenza indirizzata all'Amministrazione;
    c. cura la consegna agli uffici postali della corrispondenza in partenza dall'Amministrazione;
    d. cura lo smistamento agli uffici competenti di destinazione della corrispondenza

ricevuta dall'Amministrazione e di quella interna tra gli uffici;
   e. gestisce la casella di Posta Elettronica Certificata dell'AOO, relativamente alla posta in arrivo;
   f. gestisce il ricevimento delle gare/concorsi quando siano svolte in modalità cartacea;
4. Il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, per lo svolgimento delle attività relative al presente articolo, si avvale delle competenze tecnico/informatiche del Responsabile dei Sistemi Informativi al quale attribuisce le necessarie autorizzazioni di Amministratore di protocollo del sistema di protocollo Informatico e di gestione documentale come meglio descritti nel successivo art. 11.
5.

III - ACCESSO AL SISTEMA INFORMATICO DOCUMENTALE E PIANO PER LA SICUREZZA INFORMATICA

Art. 10 - Accessi differenziati

1. Gli operatori interni del servizio di protocollo informatico hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni.
2. Ad ogni operatore è assegnata una "login" ed una "password" d'accesso al sistema informatico di gestione del protocollo. Ogni operatore, identificato dalla propria login dal sistema informatico di gestione del protocollo, è responsabile della corrispondenza dei dati desunti dal documento protocollato con quelli immessi nel programma di protocollo, e della corrispondenza del numero di protocollo di un documento all'immagine o file del documento stesso archiviato nel sistema informatico.
3. I livelli di autorizzazione sono assegnati dal Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi secondo i principi contenuti nel presente provvedimento.
4. Gli operatori di protocollo, in base al loro livello di abilitazione, possono essere:
   a. Amministratori Protocollo
   b. Operatori di Protocollo
   c. Operatori di Protocollo uffici decentrati
   d. Operatori di Protocollo altri uffici dell'Ente

Art. 11 - Amministratore di Protocollo

L'amministratore di di protocollo ha tutte le seguenti abilitazioni consentite dal programma di gestione del protocollo informatico:

   a. registrazione di protocolli in entrata, in uscita e interni;
   b. annullamento di protocolli già registrati;
   c. modifica di protocolli già registrati;
   d. ricerca dati;
   e. visione di tutti i documenti archiviati;
   f. gestione delle tabelle degli operatori e della relativa definizione delle abilitazioni;
   g. creazione e tenuta delle login e password di tutti gli operatori.
   h. gestione e tenuta delle tabelle degli indirizzi PEC per l'inoltro della corrispondenza.

Art. 12 - Operatore di Protocollo

Gli operatori di protocollo sono tutti gli addetti della U.O. Protocollo. Le abilitazioni concesse sono:

   a. registrazione protocolli in entrata, uscita e interni;
   b. modifica/annullamento protocolli già registrati su autorizzazione del Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;

c. Ricerca dati;
d. visione di documenti archiviati.
e. smistamento successivo alle altre strutture per competenza

Art. 13 - Operatore di Protocollo uffici decentrati

Gli operatori di protocollo uffici decentrati sono i dipendenti appartenenti agli uffici che effettuano la protocollazione in sede decentrata rispetto all'U.O. Protocollo.
Le abilitazioni concesse sono:

a. registrazione protocolli in entrata per documenti inerenti le attività di competenza dell'ufficio;
b. registrazione protocolli in uscita e interni;
c. ricerca dati;
d. visione dei documenti di competenza dell'ufficio

Art. 14 - Operatore di Protocollo altri uffici dell'Ente

Gli operatori di protocollo altri uffici dell'Ente sono i dipendenti appartenenti a tutti gli uffici dell'ente che effettuano la protocollazione dei propri documenti.
Le abilitazioni concesse sono:

a. registrazione protocolli in uscita e interni per documenti inerenti le attività di competenza dell'ufficio;
b. ricerca dati;
c. visione dei documenti di competenza dell'ufficio.

Art. 15 - Piano per la sicurezza informatica

Il sistema per la Gestione del Protocollo Informatico e dei flussi documentali è un servizio software fruibile in tecnologia CLOUD/SaaS (Software as a Service) pertanto la ditta che lo fornisce :

- ne assicura la "Sicurezza fisica" ovvero la sicurezza delle apparecchiature hardware (server) all'interno delle quali è installato il software per la gestione del protocollo informatico e ne garantisce la manutenzione e tempi di intervento adeguati per il ripristino degli apparati in caso di guasti.
- ne assicura sicurezza è la "Sicurezza Logica" ovvero il sottosistema di sicurezza finalizzato alla implementazione dei requisiti di sicurezza all'interno dell'architettura informatica mediante l'attivazione di:
  a. *Meccanismi per il controllo degli accessi*. Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico documentale avvengano secondo le modalità prestabilite (login, password). Il sistema di database traccia un file di registrazione degli accessi (file di log).
  b. *Funzioni per la realizzazione dell'integrità logica*. Ogni utente, superata la fase di autenticazione, ha accesso solo ai dati residenti nella propria area di lavoro (scrivania virtuale) e non può accedere ad altre aree di lavoro.
  c. *Funzioni per la realizzazione dell'integrità fisica*. L'integrità fisica dei dati viene garantita sia da un'adeguata configurazione hardware (ridondanza server farm) sia dalle politiche del sistema di backup che prevedono la gestione di tutti i dati relativi al sistema di protocollo e gestione documentale : database, documenti e componenti applicative. Ibackup hanno frequenza giornaliera e retention/storico di 30 giorni. I job di backup non impattano l'erogazione dei servizi e avvengono a caldo sul nodo del cluste "slave"

Per ogni ulteriore dettaglio tecnico si rimanda a quando descritto nell'Allegato "F" : Piano per la sicurezza informatica

IV - IL DOCUMENTO

Art. 19 - Principi generali

1. Secondo quanto previsto dalla normativa vigente (Artt. 40 e 71 del CAD), l'Amministrazione forma i propri documenti originali come documenti informatici.
2. Al fine della gestione del documento informatico nel sistema documentale, la spedizione e la conservazione a norma dello stesso, i formati ammessi sono quelli riportati nell'allegato "B". Il documento principale è sempre in formato PDF/A firmato digitalmente.
3. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta. Per l'espletamento delle attività istituzionali, l'Amministrazione fornisce la firma digitale agli amministratori, ai dirigenti, ed ai dipendenti da essa delegati a rappresentarla.
4. Fermo restando quanto previsto al comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti indispensabile.
5. Ogni documento per essere inoltrato in modo formale, all'esterno o all'interno dell'Amministrazione:
    - deve trattare un unico argomento indicato in modo sintetico ma esaustivo, a cura dell'autore, nello spazio riservato all'oggetto;
    - deve riferirsi ad un solo protocollo;
6. Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte all'atto della sua protocollazione.
7. Il documento deve consentire l'identificazione dell'Amministrazione mittente attraverso le seguenti informazioni:
    - la denominazione, l'indirizzo completo, il codice fiscale/Partita IVA, e il logo dell'Amministrazione secondo lo specifico modello lettera in allegato "D";
    - l'indicazione completa dell'ufficio dell'Amministrazione che ha prodotto il documento corredata dai numeri di telefono, e dagli eventuali orari di apertura al pubblico.
8. Il documento, inoltre, deve recare almeno le seguenti informazioni:
    - il luogo di redazione del documento;
    - la data (giorno, mese, anno);
    - numero di protocollo se trattasi di documenti originali cartacei;
    - il numero degli allegati (se presenti);
    - l'oggetto del documento;
    - se trattasi di documento informatico, la firma digitale da parte del Responsabile del procedimento e/o del responsabile del provvedimento finale;
    - se trattasi di documento cartaceo, la sigla autografa da parte del Responsabile del procedimento e/o del Responsabile del provvedimento finale.
9. Il documento informatico, la sua registrazione su supporto informatico e la sua trasmissione con strumenti telematici sono validi e rilevante a tutti gli effetti di legge se conformi alle disposizioni del C.A.D. e regolamenti attuativi.

Art. 20 - Documenti ricevuti dall'Amministrazione

1. I documenti informatici devono essere recapitati all'Amministrazione prevalentemente:
    - a mezzo posta elettronica certificata;
    - tramite servizi di e-government on line;
    - tramite INTERPRO;
2. I documenti informatici posso essere recapitati anche su supporti di memorizzazione (cd rom, dvd, chiave usb, etc.) consegnati direttamente all'Amministrazione o inviati per

posta

convenzionale, posta raccomandata o corriere ma la loro registrazione a protocollo segue le regole di cui al successivo art. 25;

3. Il documento su supporto cartaceo può essere recapitato:
    - a mezzo posta convenzionale, posta raccomandata o corriere;
    - a mezzo consegna diretta all'Amministrazione.

Art. 21 - Documento inviato dall'Amministrazione

1. I documenti informatici, compresi gli eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica certificata.
2. In alternativa i documenti informatici, da trasmettere alle amministrazioni locali della Regione Toscana, possono essere trasmessi tramite il sistema INTERPRO.
3. Per l'invio tramite i mezzi telematici di cui ai commi precedenti di documenti informatici, compresi gli eventuali allegati, che superino, in termini di MB (MegaByte) il valore totale di 100 (> 100MB) si rimanda alle modalità operative di cui all'allegato "E";
4. I documenti su supporto cartaceo sono inviati:
    - a mezzo posta convenzionale;
    - a mezzo posta raccomandata;

Art. 22 - Documento interno formale

1. I documenti interni dell'Amministrazione sono formati con tecnologie informatiche.
2. Lo scambio tra gli uffici dell'Amministrazione di documenti informatici di rilevanza amministrativa giuridico-probatoria – quando essi non siano assistiti da procedure informatiche che ne garantiscano altrimenti la tracciabilità – avviene, di norma, per mezzo della procedura di protocollo informatico; il documento informatico scambiato viene sottoscritto con firma digitale.

Art. 23 - Documento interno informale

Per la documentazione interna informale, la cui conservazione è facoltativa, può essere utilizzato il sistema di mail, in quanto questo genere di documenti non interessa il sistema di protocollo informatico.

V - DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Art. 24 - Ricezione di documenti informatici sulla casella di posta elettronica certificata

1. La casella di PEC istituzionale è accessibile solo all'U.O. Protocollo, che procede alla registrazione di protocollo.
2. Qualora il messaggio di posta elettronica non sia conforme agli standard indicati dalla normativa vigente, se possibile si procederà comunque alla protocollazione. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quella di una missiva non sottoscritta e comunque valutabile dal Responsabile del procedimento.
3. La verifica della validità e autenticità della eventuale firma digitale o elettronica apposta, della provenienza e integrità dei documenti stessi della leggibilità e della conformità del documento è a carico dell'ufficio destinatario interno.

Art. 25 - Ricezione di documenti informatici su supporti di memorizzazione

1. L'Amministrazione si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto di memorizzazione, analogamente a quanto previsto dall'art. 24 in termini di integrità e leggibilità.
2. Verrà associato alla registrazione di protocollo solo il documento informatico (lettera di

accompagnamento) contenuto nel supporto di memorizzazione il restante contenuto non verrà associato alla registrazione di protocollo. Si assicura la consegna del supporto di memorizzazione all'ufficio destinatario

Art. 26 - Ricezione di documenti cartacei

1. L'U.O. Protocollo provvede a ritirare la corrispondenza quotidiana consegnata dagli operatori dei servizi postali e dai corrieri.
2. La consegna "brevi manu" direttamente dall'utenza viene effettuata presso lo sportelli predisposto presso la U.O. Protocollo.
3. Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti, e successivamente aperti per gli ulteriori controlli preliminari alla registrazione di protocollo; la busta o contenitore si allega al documento per la parte relativa ai timbri postali.

Art. 27 - Documenti cartacei ricevuti e tutela dei dati personali

1. Il personale preposto all'apertura e alla registrazione della corrispondenza è regolarmente autorizzato al trattamento dei dati personali in qualità di "incaricato al trattamento" seguendo le modalità gestionali descritte nel presente MdG.
2. Qualora la corrispondenza riservata e/o personale venga recapitata per errore ad un ufficio dell'Amministrazione quest'ultimo, a tutela dei dati personali eventualmente contenuti, non apre le buste o i contenitori e li rinvia, nella stessa giornata, alla U.O.Protocollo che provvede alla restituzione al mittente secondo le modalità descritte nel successivo art. 29.

Art. 28 - Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta elettronica certificata istituzionale dell'AOO messaggi e relativi allegati 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 QUESTO COMUNE".

Art. 29 - Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente all'U.O. Protocollo corrispondenza indirizzata ad altri soggetti le buste o i contenitori si restituiscono a Poste Italiane. Qualora la busta o il contenitore venga aperto per

errore si provvede a richiuderà la busta e si invia al mittente apponendo sulla busta la diciture "PERVENUTO ED APERTO PER ERRORE".

Art. 30 - Rilascio di ricevute attestanti la ricezione di documenti informatici

1. Nel caso di ricezione di documenti informatici mediante la casella di posta elettronica certificata, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell'AOO.
2. Qualora si ritenga necessario, o se richiesto dal mittente, è possibile restituire al mittente la ricevuta contenente il numero di protocollo assegnato al documento informatico pervenuto.

Art. 31 - Rilascio di ricevute attestanti la ricezione di documenti cartacei

1. Per i documenti soggetti a protocollazione, quando il documento cartaceo è consegnato "brevi manu" ed è richiesto il rilascio di una ricevuta, la U.O. Protocollo che lo riceve deve rilasciare, almeno, la ricevuta attestante l'avvenuta consegna provvedendo ad effettuare una copia fotostatica del frontespizio del documento e apponendo il timbro dell'Amministrazione con la data e l'ora d'arrivo ed eventuale sigla dell'operatore.

2. La semplice apposizione del timbro dell'Amministrazione con la data e l'ora d'arrivo ed eventuale sigla dell'operatore sulla copia non ha alcun valore giuridico.

Art. 32 - Assegnazione telematica dei documenti

1. I documenti ricevuti in via telematica sono resi disponibili agli uffici dell'Amministrazione, attraverso procedura informatica, subito dopo l'operazione di protocollazione e di assegnazione.
2. I documenti ricevuti su supporto cartaceo, di formato inferiore od uguale all'A4, dopo le operazioni di registrazione e segnatura protocollo, sono acquisiti in formato PDF/A con l'ausilio di scanner da tavolo e/o massivi e resi disponibili agli uffici dell'Amministrazione attraverso procedura informatica. I documenti cartacei originali vengono trasmessi agli uffici competenti.
3. I documenti ricevuti su supporto cartaceo di formato diverso da A4 vengono trasmessi agli uffici competenti esclusivamente su supporto cartaceo, comunque dopo le operazioni di registrazione e segnatura di protocollo su procedura informatica ed acquisizione a scanner del solo frontespizio.

Art. 33 - Presa in carico dei documenti

L'ufficio di destinazione esegue una verifica di congruità in base alle proprie competenze, esegue l'operazione di presa in carico e lo inserisce nel fascicolo informatico di destinazione.

Art. 34 - Registrazioni di protocollo e segnatura

Le operazioni di registrazione e di apposizione della segnatura del documento in partenza sono effettuate da ciascun ufficio dell'Amministrazione.

Art. 35 - Verifica formale dei documenti da spedire

1. Gli uffici mittenti dell'Amministrazione sono responsabili della verifica formale dei requisiti essenziali ai fini della spedizione (ad esempio: corretta indicazione del destinatario; sottoscrizione, presenza di allegati se dichiarati, etc.)
2. Tutti la documentazione amministrativa cartacea da spedire, è inoltrata all'U.O. Protocollo già protocollata e recante la segnatura di protocollo.
3. In nessun caso gli operatori della U.O. Protocollo sono tenuti a prendere cognizione del contenuto dei documenti da spedire e quindi essi non devono operare alcun controllo nel merito dei contenuti dei documenti stessi.

Art. 36 - Spedizione di documenti informatici

1. I documenti informatici da inviare all'esterno dell'Amministrazione devono essere trasmessi, a cura degli uffici interni mittenti, previa la verifica di cui al precedente articolo 35, tramite Posta elettronica certificata o INTERPRO.
2. Per la trasmissione deve essere usata come casella PEC l'indirizzo istituzionale comune.massa@postacert.toscana.it, le relative ricevute di accettazione e di avvenuta consegna sono assicurate ed associate alla registrazione di protocollo dal sistema di protocollo informatico.

Art. 37 - Spedizione di documenti cartacei a mezzo posta

L'U.O. Protocollo provvede direttamente a tutte le operazioni necessarie alla spedizione della corrispondenza. Al fine di consentire il regolare svolgimento di tali operazioni gli uffici dell'Amministrazione devono far pervenire la posta in partenza all'U.O. Protocollo nelle ore stabilite dall'Ufficio stesso. Eventuali situazioni di urgenza saranno valutate dal Responsabile Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi che potrà autorizzare, in via eccezionale, procedure diverse da quella standard

descritta.

Art. 38 - Ricezione di documenti tramite telefax e telegramma

Il documento ricevuto tramite telefax sono trasmessi agli uffici destinatari trami eMail integrata nella gestione informatica del Fax comunale.

I telegrammi ricevuti dall'Amministrazione non vengono protocollati ma consegnati all'ufficio destinatario in forma cartacea, è a cura dello stesso, se lo ritiene opportuno, inviarli alla U.O. Protocollo per la loro registrazione a protocollo.

Art. 39 - Ricevute di trasmissione raccomandate AR

La U.O. Protocollo cura l'invio delle ricevute di ritorno all'ufficio interno mittente che si fa carico di archiviarle nel relativo fascicolo.

VI - REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI RICEVUTI

Art. 40 - Regole generali

1. L'assegnazione avviene "per competenza" ad un'unico Settore/Servizio/Ufficio responsabile del procedimento e può essere trasmesso anche ad altri Settori/Servizi/Uffici ritenuti interessati.
2. Nel caso di assegnazione errata, l'ufficio che riceve il documento, lo restituisce all'Ufficio Protocollo per consentire di procedere ad una nuova assegnazione.
3. I termini per la definizione del procedimento amministrativo che, eventualmente, prende avvio dal documento, decorrono, comunque, dalla data di protocollazione.
4. Il sistema di gestione informatica dei documenti memorizza tutti i singoli passaggi conservandone, per ciascuno di essi, l'identificativo dell'operatore, la data e l'ora di esecuzione.
5. La traccia risultante dalle operazioni di cui al comma precedente definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

VII - DOCUMENTI ESCLUSI DALLA REGISTRAZIONE

Art. 41 - Documenti esclusi dalla registrazione di protocollo

Le tipologie di documenti esclusi dalla registrazione di protocollo sono riportate nell'allegato "C" del presente MdG.

VIII - MODALITA' DI PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Art. 42 - Unicità del protocollo informatico

1. Nell'ambito della AOO l'Amministrazione istituisce un unico registro di Protocollo Generale.
2. La numerazione progressiva delle registrazioni di protocollo è unica, si chiude al 31 dicembre di ogni anno e ricomincia dal 1° gennaio dell'anno successivo.
3. Ai sensi della normativa vigente, il numero di protocollo è costituito da almeno sette cifre numeriche; esso individua un solo documento e, pertanto, ogni documento deve recare un solo numero di protocollo.
4. Non è consentita la protocollazione di 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.

5. Non è consentita, in nessun caso, la cosiddetta “registrazione a fronte”, vale a dire l’utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
6. Il registro di protocollo è un atto pubblico che fa fede dell’effettivo ricevimento o spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici; esso, pertanto, è soggetto alle forme di pubblicità e di tutela delle situazioni giuridicamente rilevanti previste dalle norme.

Art. 43 - Registrazioni di protocollo

1. Ai sensi della normativa vigente (Art. 21 comma 1 lettera d) del D.lgs 42/2004) e con le eccezioni previste dal presente MdG, su ogni documento ricevuto o spedito dall’AOO e sui documenti interni formali, viene effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei seguenti dati obbligatori:
    - il numero di protocollo, generato automaticamente dal sistema è registrato in forma non modificabile;
    - la data di registrazione di protocollo, assegnata automaticamente dal sistema è registrata in forma non modificabile;
    - il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
    - l’oggetto del documento, registrato in forma non modificabile;
    - la data e il numero di protocollo del documento ricevuto, se disponibili;
    - 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’ufficio competente
2. La registrazione di protocollo di un documento informatico viene effettuata a seguito delle procedure previste al Capo V del presente regolamento.
3. La registrazione di protocollo di un documento cartaceo viene effettuata a seguito delle procedure previste al Capo V del presente regolamento.

Art. 44 - Elementi facoltativi delle registrazioni di protocollo

1. La registrazione di protocollo di un documento, oltre ai dati obbligatori di cui al precedente articolo 57, può contenere i seguenti elementi facoltativi:
    - la classificazione del documento;
    - il mezzo di ricezione/spedizione del documento (ad esempio: raccomandata o fax);
    - il collegamento ad altri documenti;
    - il riferimento agli allegati;
    - il nominativo dei destinatari delle copie per conoscenza;

2. In caso di errore di registrazione gli elementi facoltativi di cui al comma precedente sono modificabili senza ricorrere alla procedura di cui al successivo articolo 60, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Art. 45 - Segnatura di protocollo dei documenti

1. La segnatura di protocollo è l’apposizione o l’associazione all’originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
2. L’operazione di segnatura di protocollo è effettuata contemporaneamente all’operazione di registrazione di protocollo.
3. I dati della segnatura di protocollo di un documento informatico sono contenuti in un file

conforme alla specifiche tecniche previste dalla normativa vigente.

4. La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un segno grafico il quale, di norma, è realizzato con un'etichetta autoadesiva corredata da codice a barre o, in alternativa, con un timbro tradizionale.
5. La segnatura di protocollo sia per i documenti informatici che per quelli cartacei deve contenere obbligatoriamente, ai sensi della normativa vigente 21, le seguenti informazioni:
6. codice identificativo dell'AOO;
7. data e numero di protocollo del documento.
8. Ad integrazione degli elementi obbligatori di cui al precedente comma 5, la segnatura di protocollo può contenere le seguenti informazioni facoltative:
    - denominazione dell'AOO;
    - ufficio ricevente
    - indice di classificazione.
9. L'acquisizione dei documenti cartacei in formato immagine pervenuti all'Amministrazione (IN ARRIVO) è effettuata solo dopo che l'operazione di segnatura di protocollo è stata eseguita in modo da acquisire con l'operazione di scansione, come immagine, anche la segnatura sul documento; le segnatura deve essere apposto sulla prima pagina dell'originale.
10. L'acquisizione dei documenti cartacei in formato immagine inviati dall'Amministrazione (IN USCITA/INTERNO) è effettuata contestualmente alla registrazione di protocollo. Al termine della registrazione di protocollo e la segnatura deve essere apposta sulla prima pagina dell'originale.

Art. 46 - Annullamento delle registrazioni di protocollo

1. Ai sensi della normativa vigente (Art. 8 "Regole tecniche Protocollo Informatico" DPCM 03/12/2013), l'annullamento e/o la modifica anche di uno solo dei dati obbligatori della registrazione di protocollo di cui al comma 1 del precedente art. 57 devono essere richieste, con specifica nota motivata, al Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi o suoi delegati che sono i soli che possono autorizzare lo svolgimento delle relative operazioni;
2. 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.
3. L'annullamento anche di una sola delle informazioni di protocollo comporta il contestuale annullamento di tutta la registrazione di protocollo.

Art. 47 - Documenti con più destinatari

Le circolari, le disposizioni generali e tutte le altre comunicazioni interne che abbiano più destinatari si registrano con un solo numero di Protocollo Generale;

Art. 48 - Corrispondenza consegnata con ricevuta

In casi particolari la corrispondenza in arrivo (es. raccomandata personale) viene consegnata agli uffici interni di destinazione, previa firma di ricevuta firmata da un addetto alla ricezione, appositamente predisposta dall'ufficio protocollo.

Art. 49 - Documenti anonimi o non firmati

I documenti anonimi non sono sottoposti alla registrazione di protocollo. Le lettere prive di sottoscrizione o prive di firme leggibile dalle quali non è identificabile il mittente non sono sottoposte a registrazione di protocollo.

Art. 50 - Corrispondenza personale o riservata

1. La corrispondenza personale è regolarmente aperta dall'ufficio protocollo per la registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura RISERVATA", "PERSONALE", o formula equivalente;
2. La corrispondenza recante la dicitura "RISERVATA" , "PERSONALE" o formula equivalente viene consegnata in busta chiusa al destinatario, previa firma di ricevuta di cui al precedente articolo 65.
3. Il destinatario, se reputa che i documenti ricevuti debbano essere, comunque, protocollati, provvede a inoltrarli alla U.O. Protocollo per le operazioni di registrazione, segnatura di protocollo e assegnazione.

IX - MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA

Art. 51 - Registro di emergenza

1. Il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi o, in caso di sua assenza, altro incaricato, autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo sul registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica.
2. Ogni ufficio che effettua la protocollazione in sede decentrata è dotato di un proprio registro di emergenza. Il registro di emergenza inizia il 1° gennaio e si chiude il 31 dicembre di ogni anno. I numeri dei protocolli del registro di emergenza sono preceduti da apposito codice identificativo assegnato dal Responsabile del Servizio di Protocollo.
3. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.
4. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, il Responsabile per la tenuta del protocollo 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 manuale è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente.
5. Nel registro di emergenza sono protocollati in via prioritaria i documenti per i quali riveste rilevanza l'effettiva data di ricevimento o di partenza. Per gli altri documenti si può procedere al differimento delle operazioni di registrazione fino al momento del ripristino della funzionalità del sistema.
6. Entro dieci giorni dal ripristino della funzionalità del sistema, le informazioni relative ai documenti protocollati manualmente sono inserite nel sistema informatico associando loro il numero di Protocollo Generale. In questo caso il documento sarà registrato con due numeri diversi:
    - l'efficacia giuridico-probatoria sarà garantita dal numero del registro di emergenza
    - il numero di Protocollo Generale garantirà l'unicità delle registrazioni.

X - NORME GENERALI PER LA PRESENTAZIONE DI PRATICHE DEMATERIALIZZATE

Art. 52 - Modalità di invio telematico

1. L'invio telematico di istanze o di comunicazioni relative ai procedimenti amministrativi può avvenire mediante le seguenti modalità:

Utilizzo di un servizio dedicato on-line appositamente predisposto sul sito del

Comune. In questo caso l'istanza /comunicazione è valida:

- se sottoscritta mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato
- ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi
- ovvero tramite il sistema pubblico di identità digitale (SPID)
- ovvero quando l'autore è identificato dalle credenziali (user_name/password) rilasciate dal Comune di Massa consegnate previa specifica richiesta di rilascio e conseguente riconoscimento personale.
- trasmesse dall'autore mediante la propria casella di posta elettronica certificata all' indirizzo PEC del Comune di Massa salvo altra disposizione appositamente regolamentata

2. Qualora l'istanza o la comunicazione venga inviata mediante posta elettronica certificata, l'oggetto del messaggio dovrà contenere tutti gli elementi necessari ad individuare in modo univoco il contenuto.
3. Qualora le dimensioni complessive del materiale da trasmettere siano eccessive e tali da richiedere l'invio di più messaggi consecutivi, l'oggetto del messaggio dovrà contenere tutti gli elementi necessari ad individuare in modo chiaro ed univoco il contenuto.
4. Qualora, in relazione ad una medesima istanza, si effettuino invii successivi degli stessi documenti via posta elettronica certificata, l'invio successivo si intende ad integrazione o in sostituzione degli invii precedenti in base alle dizioni contenute nel nuovo messaggio.
5. Le regole tecniche di cui ai precedenti commi saranno costantemente aggiornate al fine di tener conto delle nuove tecnologie e delle normative specifiche in tema di formati dei documenti digitali.

XI - NORME FINALI

Art. 53 - Pubblicità del presente manuale

1. Il presente MdG è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.
2. Il presente MdG è pubblicato sul sito internet dell'amministrazione.

Art. 54 - Entrata in vigore

Il presente MdG entra in vigore il primo giorno del mese successivo a quello della sua approvazione.

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

ALLEGATO "A" - DESCRIZIONE DELL'Area Organizzativa Omogena (AOO)

Denominazione dell'AOO
COMUNE DI MASSA

Codice identificativo AOO sull'Indice delle Pubbliche Amministrazioni (IPA)
c_f023

Data di accreditamento AOO all'IPA
01/06/2010

Nominativo del Responsabile del Servizio di Protocollo Informatico, gestione dei flussi documentali e degli archivi
Dott. Massimo Dalle Luche
Dirigente del Settore Servizi di STAFF e Generali
massimo.dalleluche@comune.massa.ms.it

Casella di Posta Elettronica Certificata
comune.massa@postacert.toscana.it

Indirizzo della sede principale dell'AOO a cui indirizzare la corrispondenza convenzionale
Comune di Massa – Via Porta Fabbrica, 1 – 54100 MASSA

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

ALLEGATO "B" - I FORMATI IDONEI PER LA FORMAZIONE/RICEZIONE DEI DOCUMENTI

1. Introduzione

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

I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.

Il presente allegato, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e allineato con la pubblicazione dell'Agenzia per l'Italia digitale.

2. I formati

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

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

2.1 Le tipologie di formato

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione.

Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

Per esigenze lavorative gestionali possono essere trattati documenti in formati diversi da quelli indicati al paragrafo 2.3, come ad esempio in formato WORD (.doc), EXCEL (.xls), POWER POINT (.ppt), purché accompagnati dalla versione dello stesso documento in uno dei formati accettati, preferibilmente PDF/A.

2.2 Caratteristiche generali dei formati

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

In particolare devono soddisfare quanto previsto da AGID

- apertura
- sicurezza
- portabilità
- funzionalità
- supporto allo sviluppo
- diffusione

2.2.1 Apertura

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

Questa condizione si verifica sia quando il formato è documentato e pubblicato da un

produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti.

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

2.2.2 Sicurezza

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

2.2.3 Portabilità

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

2.2.4 Funzionalità

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

2.2.5 Supporto allo sviluppo

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

2.2.6 Diffusione

La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici.

Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Inoltre nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

2.3 Formati idonei per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.

In particolare è necessario tener conto nella scelta dei seguenti elementi:

- non devono poter contenere macroistruzioni o codici eseguibili, ovvero devono essere disponibili gli strumenti capaci di rilevarne la presenza con sufficiente sicurezza;
- devono essere standard e documentati, ovvero le relative specifiche devono essere pubblicamente accessibili, complete ed esaustive;
- devono essere robusti, accurati, ampiamente adottati ed usabili
- devono essere indipendenti dalle piattaforme tecnologiche, in modo da poter visualizzare un documento senza particolari vincoli di natura informatica o il pagamento di royalty;
- devono essere conformi alle disposizioni emanate dalle autorità competenti in materia di archiviazione e conservazione digitale.

Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti informatici.

Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione

previsto dalla normativa per le singole tipologie di documenti informatici.

I formati di seguito indicati sono un primo elenco di formati da usare per la conservazione:

- **PDF/A (Portable Document Format/Archive)** formato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali.
- **ODF (Open Document Format)** è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione.
- **XML (Extensible Markup Language)** formato di testo flessibile. E' un linguaggio di markup, ovvero un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.
- **OOXML (Office Open XML)** è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.
- **TXT** è un file che contiene solo caratteri di scrittura semplici, che compongono un testo leggibile direttamente dagli utenti senza bisogno di installare programmi appositi.
- **RTF (Rich Text Format)** è un file ASCII con stringhe di comandi speciali in grado di controllare le informazioni riguardanti la formattazione del testo: il tipo di carattere e il colore, i margini, i bordi del documento, ecc.
- **TIFF (Tagged Image File Format)** formato immagine di tipo raster.
- **DXF (Drawing Interchange Format, o Drawing Exchange Format),** un formato simile al DWG(Autocad) , di cui sono state rilasciate le specifiche tecniche.
- **Shapefile** un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con con i prodotti che usano i precedenti formati. Il formato è stato sviluppato e regolato da ESRI, allo scopo di accrescere l'interoperabilità fra i sistemi ESRI e altri GIS. Di fatto è diventato uno standard per il dato vettoriale spaziale, e viene usato da una grande varietà di sistemi GIS.
- **SVG (Scalable Vector Graphics**), un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

Come già indicato nelle premesse questo elenco sarà periodicamente aggiornato, sulla base delle nuove tecnologie e dei nuovi standard definiti da AGID.

Qualora detta documentazione debba possedere specifiche valenze giuridiche, tra cui ad esempio l'opponibilità a terzi, deve essere prodotta nei formati indicati nei punti precedenti, o altri che offrano analoghe o maggiori garanzie a motivo dell'evoluzione tecnologica, e firmata digitalmente.

Per i formati indicati deve essere garantita dagli applicativi informatici, la corretta visualizzazione dei contenuti. Date le caratteristiche richieste per i documenti informatici in tema di inalterabilità e immutabilità, non sono accettati né trasmessi file compressi, come ad esempio i file con estensione ".ZIP" oppure ".RAR". I documenti informatici prodotti dall'Amministrazione su formati diversi (ad esempio, in estensione ".doc" di Microsoft Word, ".xls" di Microsoft Excel) prima della loro sottoscrizione con firma elettronica o comunque nel momento che si considerano perfezionati, sono convertiti nel formato PDF/A - o nei formati sopraindicati se maggiormente confacenti al tipo di documento considerato - al fine di garantirne la leggibilità, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

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

ALLEGATO “C” - (ELENCO DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO)

Si riporta, innanzitutto, il testo del comma 5 dell’art. 53 del D.P.R. 28.12.2000, n. 445, che recita: “*Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall’amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i 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 e tutti i documenti già soggetti a registrazione particolare dell’amministrazione*”.

Inoltre, sono escluse dalla protocollazione le seguenti categorie di documenti:
• Le comunicazioni d’occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
• Le richieste di ferie ed altri permessi ad esclusione dei permessi sindacali;
• Le richieste di rimborso spese e missioni;
• I certificati di malattia;
• I certificati di infortunio;
• La pubblicità conoscitiva di convegni;
• La pubblicità in generale;
• Le offerte, i listini prezzi e i preventivi di terzi non richiesti;
• Le ricevute di ritorno delle raccomandate A.R.;
• Le convocazioni ad incontri o riunioni interne;
• I curricula non richiesti;
• I cosiddetti “ritorni”, cioè le risposte alle richieste di certificazioni varie avanzate dall’Amministrazione a vari enti, i quali rispondono apponendo semplicemente sulla richiesta medesima diciture o timbri quali “Nulla” o “Nulla osta”, ecc.;
• Tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico-amministrativa presente o futura.

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

ALLEGATO "D" - Modello di lettera del Comune di Massa INTESTAZIONE

COMUNE DI MASSA
Settore XXXXXXXXXXXXXXX
Servizio xxxxxxxxxxxxxxxxxxx
Via xxxxxxxxxxxxx , xx

PIE' DI PAGINA

Comune di Massa, Via Porta Fabbrica, 1 – 54100 Massa – centralino 0585 4901 – Sito web www.comune.massa.ms.it – Codice fiscale e Partita IVA : 00181760455 - Codice univoco ufficio per la fatturazione elettronica: UFCQTV

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

ALLEGATO “E” - (MODALITA’ OPERATIVE TRASMISSIONE TRAMITE PEC/INTERPRO DI DOCUMENTI INFORMATICI “PESANTI”)

In considerazione del fatto che le caselle di Posta Elettronica Certificata presentano limiti di ricezione/invio di documenti informatici codidetti “pesanti” ovvero che, in totale, superino una dimensione in termini di MB (Mega Byte) superiore a 100 (> 100MB) si descrivono di seguito le modalità operative con le quali gli uffici possono trasmetterli.

1. l’ufficio raccoglie ed inserisce in un supporto di memorizzazione (cd, dvd, chiavetta USB) tutti i documenti.
2. avvisa, per tempo, i sistemi informativi di tale necessità
3. i sistemi informativi, ricevuto i suddetto supporto di memorizzazione procedono come di seguito descritto :
    a. provvedono a generare una cartella compressa (file .zip) contenete tutti i documenti contenuti nel supporto di memorizzazione
    b. trasferiscono la cartella compressa in una sezione riservata del sito web comunale
    c. provvedono a generare la URL (collegamento ipertestuale) alla cartella compressa attraverso il quale sarà possibile scaricarla
    d. provvedono a generare le credenziali di accesso necessarie per scaricare la cartella compressa
    e. provvedono a generare la codifica SHA (Secure Hash Algoritm) della cartella compressa che corrisponde all’impronta digitale univova della stessa ovvero una sequenza di caratteri alfanumerici che è sempre diversa per documenti diversi (non possibile, con la tecnologia attuale, generare due codifiche hash uguali per file diversi)
    f. foriniscono tramile mail all’ufficio le informazioni di cui ai punti c,d,e

4. l’ufficio provvede a redigere un documento informatico di trasmissioni in cui riporta le informazioni ricevute indicando che i documenti digitali sono scaricabili dalla URL indicata
5. l’ufficio protocolla e invia tramite pec al destinatario il documento informatico di cui al punto

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

ALLEGATO "F" - Piano per la sicurezza informatica

Il sistema di protocollo informatico e gestione documentale di seguito **SPIGD** ricompresso nella piattaforma tecnologica URBI Smart in uso presso il Comune di massa è accessibile da qualsiasi dispositivo mobile (essendo web nativo, si "muove" agevolmente in Internet) e in qualsiasi momento e luogo grazie alla modalità **CLOUD COMPUTING - di seguito Cloud -** definita anche SAAS (Software as a service). L'architettura web nativa – con accesso mediante qualsiasi PC con browser collegato a Internet o anche attraverso i più moderni strumenti mobile (come ipad Apple, tablet con Android oltre che iPhone, smartphone, palmari ecc.) – consente una naturale predisposizione verso il Cloud. Ill **SPIGD** quindi si trova nella "nuvola informatica" (essendo in rete) e non risiede presso i server dell'ente che ne fruisce, ma in server dislocati presso un Internet Data Center (IDC) esterno sul territorio nazionale italiano.
Oltre ad essere in linea con le direttive dell'Agenzia per l'Italia Digitale (ex Digit PA, già CNIPA), tale modalità di erogazione consente di utilizzare soluzioni ad alto profilo tecnologico e costantemente aggiornate, protette e in grado di facilitare notevolmente l'interazione con i cittadini o altri soggetti esterni, senza forti investimenti infrastrutturali e pesanti costi di gestione (ad es. acquisto di software, hardware e infrastrutture di rete, costi di personale altamente specializzato per la gestione di infrastrutture complesse necessarie per usufruire della rete ecc.). L'ente si avvale così anche **di un servizio specializzato che consente il ripristino rapido e completo dei dati in caso di interruzioni impreviste dei servizi e, quindi, la continuità operativa dei propri utenti** (in linea con quanto disposto dall'art. 50 del D. Lgs. 82/2005, Codice dell'Amministrazione Digitale - CAD). La tecnologia web rende il **SPIGD** estremamente efficace

Cloud: vantaggi

L'utilizzo del **SPIGD** in modalità Cloud, oltre alla possibilità di accedere ovunque alle applicazioni, consente di avere molti vantaggi:

- Nessuna necessità di competenza informatica per la gestione di hardware, software e degli archivi.
- Nessun limite connesso alla necessità di dimensionamento del sistema: non occorre infatti stabilire a priori il dimensionamento dell'hardware, dato che, anche al crescere delle esigenze occorre esclusivamente aggiungere i posti di lavoro utente necessari.
- Nessun vincolo hardware e software.
- Totale eliminazione della responsabilità di archiviazione dei dati.
- Nessun vincolo contrattuale per l'eventuale cambio di fornitore.
- Estrema scalabilità.
- Aggiornamenti del software applicativo immediatamente disponibili.
- Supporto garantito con tempi di risposta velocizzati da un servizio help desk che può intervenire tramite l'attivazione del servizio di assistenza da remoto che, sfruttando il collegamento Internet, può operare sul PC del cliente (previo consenso per l'accesso) ed effettuare la corretta diagnostica al fine di apportare le operazioni correttive.

Sicurezza dei dati e continuità operativa

Il servizio Cloud del **SPIGD** è erogato attraverso un Internet Data Center certificato in base al vigente standard internazionale ISO/IEC 27001 e alle estensioni ISO/IEC 27017 e ISO/IEC 27018, all'interno del quale le apparecchiature per la trasmissione dei dati e le architetture hardware/software preposte all'erogazione dei servizio sono poste in condizioni di massima **sicurezza applicativa e fisica** (sistemi antintrusione, sistemi

antincendio, controllo accessi, telesorveglianza ai piani; ridondanza dei sistemi elettrici e di refrigerazione), **informatica e logica** (sistemi antintrusione).
Relativamente alla sicurezza fisica e infrastrutturale, l'Internet Data Center è dotato di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. I sistemi di backup dei dati, il Disaster Recovery, la continuità dei servizi, offrono agli utenti i più elevati livelli di servizio, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tali garanzie sono fondamentali e indispensabili per rispondere agli obblighi di legge in materia di **Business Continuity** (già citato art. 50, D. Lgs. 82/2005 - CAD).
La sicurezza fisica del **SPIGD** è garantita un servizio di **Disaster Recovery** completamente automatizzato in tutti i suoi processi e monitorato da personale tecnico specializzato 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tutti i sistemi ed apparati di rete/strutturali sono in configurazione fault-tolerance per evitare Single Point of Failure. La capacità di elaborazione del sistema di Disaster Recovery permette, in caso di disastro, il ripristino dell'erogazione dei servizi con prestazioni equivalenti al sito di normale operatività, in tempi conformi al Tier 3 e a quanto indicato al paragrafo successivo "*Servizi di backup e Disaster Recovery"*. Le

Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi. Il sito primario di erogazione servizi Cloud è presso il Data Center di Westpole SpA, in Via Francesco Sforza 13, Basiglio (MI). Il sito secondario di Disaster Recovery è presso il Data Center di Westpole SpA in Via della Civiltà del Lavoro 52, Roma.

Internet Data Center

Le reti Metropolitane per i due Data Center (sito primario e sito secondario, citati al paragrafo precedente) si basano sulla cablatura in fibra la cui banda complessiva è di alcuni Gbps con possibilità di ampliamento immediato senza modifiche infrastrutturali. Il collegamento verso la rete pubblica internet viene garantito attraverso router di backbone con attestati i link di diversi operatori. Il protocollo di routing BGPV4, costantemente gestito sui router di backbone, decide le destinazioni selezionando il carrier con la miglior qualità di servizio da e verso specifiche aree geografiche. In caso di disservizio di uno dei carrier, il BGP provvede automaticamente a instradare tutto il traffico verso l'operatore funzionante e, se necessario, anche transitando per la connettività attestata sul sito secondario rispetto al Data Center che sta erogando il servizio. I due Data Center sono connessi tra di loro da una dorsale in fibra, permettendone la gestione come fosse un "unico" Data Center distribuito. Il sistema di controllo degli accessi prevede una postazione di guardiania che identifica il personale che richiede accesso e fornisce badge che consente l'accesso alle sole aree di pertinenza.

Infrastruttura di sistema

L'**architettura del Data Center** è basata su componenti le cui principali caratteristiche sono:
- utilizzo di sole componenti di classe Enterprise;
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità effettiva dell'infrastruttura presenta un uptime del 99.95%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate. Per garantire la massima disponibilità e fruibilità delle risorse atte all'erogazione dei servizi in modalità Cloud, PA Digitale monitora periodicamente le proprie risorse infrastrutturali predisponendo un Piano di Capacità/Capacity Plan con revisione minima annuale. Scopo del Piano è dunque assicurare in ogni momento la capacità sufficiente per garantire il più alto livello di erogazione dei servizi in Cloud, in base alle attuali e future esigenze di

business del mercato. Il piano viene inoltre aggiornato in seguito a cambiamenti significativi del personale, dell'organizzazione o delle infrastrutture.

Sottosistema di virtualizzazione

I servizi per il **SPIGD** sono erogati da un cluster di sistemi ad alta affidabilità VMware Enterprise in regime di Private Cloud, con risorse computazionali dedicate al fine di prevenire condivisione di risorse con altri ambienti. Alcune delle caratteristiche salienti:

- Vmotion: consente di migrare real time le VM tra host fisico ad un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su **SAN ad alte prestazioni dedicate al servizio**.

La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hardware senza completo fermo del sistema. Le garanzie:

- **alta affidabilità dei componenti fisici**, tutti i componenti sono ridondati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- **scalabilità verticale ed orizzontale dell'infrastruttura** che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall è implementata utilizzando **due firewall in cluster HA**, per la gestione dell'accesso internet e per la gestione della DMZ e LAN interna.

I server applicativi utilizzano **VLAN** per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.

L'infrastruttura dispone di **sonde IPS** (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service), di sonde antivirus per l'analisi di tutto il traffico web e per prevenire l'eventuale infezione causata da malware.

La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di password a criptazione forte.

L'accesso ai sistemi, da parte della ditta che garantisce il servizio, per scopi di amministrazione avviene attraverso connessioni **VPN** autenticate attraverso username/password e certificati digitali.

Politiche di backup

Le politiche di backup adottate prevedono la gestione di tutti i dati relativi a Urbi Smart 2020: database, documenti e componenti applicative. I backup hanno frequenza giornaliera e retention/storico di 30 giorni. I job di backup non impattano l'erogazione dei servizi, i backup dei database avvengono a caldo sul nodo del cluster "slave".

Servizi di backup e Disaster Recovery

La strategia di backup adottata per l'adozione delle Politiche descritte al punto precedente, prevede l'implementazione e l'utilizzo di Veeam Backup and Replication e di NAS Platform Snapshots.

Le soluzioni adottate permettono il recupero dei dati, garantendone un corretto processo di ripristino e l'identificazione dei dati necessari recuperando il supporto di backup appropriato.

Sono pianificate delle prove di ripristino dei dati in maniera randomica, che consistono nel

restore di un ambiente virtuale in un'area di test e le relative verifiche di buon funzionamento. La granularità dei backup relative ai database consente il recupero a livello del singolo record ad una data specifica.
Il Disaster Recovery è gestito con tecnologia VMware Site Recovery Manager. Il sistema garantisce una procedura di disaster recovery con RPO di 4 ore ed RTO minimo di 8 ore e massimo di 48 ore.

La gestione della sicurezza e sistemi di security management per le procedure applicative

La gestione della sicurezza costituisce una tra le componenti più delicate nell'ambito, più generale, della gestione dei dati dei Clienti.
Dovendo implementare un IDC per l'erogazione dei servizi di amministrazione degli enti in modalità Cloud, la ditta che garantisce il servizio per il da parte della ditta che garantisce il servizio ha da tempo sviluppato e attuato una metodologia per l'analisi dei rischi legati alla sicurezza e alla sua gestione attraverso opportuni meccanismi e strumenti di controllo e di intervento.
Le scelte adottate, in linea con quanto enunciato dall'Agenzia per l'Italia Digitale in materia di sicurezza, portano a:
- controllo e monitoraggio degli accessi in modo puntuale e nel tempo;
- identificazione di eventuali anomalie;
- intervento nel minor tempo possibile per ripristinare la situazione correttamente.

Principi applicabili al legittimo trattamento dei dati

Per soddisfare i requisiti di sicurezza, il software gestionale Urbi Smart 2020 osserva principi applicabili al legittimo trattamento dei dati (con particolare riguardo verso le Informazioni Personali Identificabili - PII), supportando una serie di servizi e di dispositivi atti ad implementare funzioni di autenticazione, autorizzazione e crittografia. Tali servizi e dispositivi risultano adeguati alla nuova normativa UE 2016/679 in vigore dal 25.05.2018, così come disposto in Italia dal Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".
L'**autenticazione** prevede che gli utenti si debbano identificare con una serie nota di credenziali, ad esempio nome utente e password.
Per **autorizzazione**, invece, si intende l'assegnazione di determinati livelli di accesso al sistema, che si riflettono in ben identificate capacità operative sul sistema medesimo da parte del singolo utente correttamente identificato.
L'attribuzione dei privilegi degli utenti, intesi come regole sia di autenticazione che di autorizzazione, sono esclusivamente demandate all'Amministratore applicativo.
Quest'ultimo può decidere se applicare su altri utenti i privilegi che regolano le policy di sicurezza, di accesso, visibilità e gestione dei dati.
La **sicurezza** dei dati è garantita:
- durante la fase di comunicazione client e server tramite utilizzo di protocollo https e crittografia di tipo TLS/SSL
- nello storage all'interno del database
- durante la fase di comunicazione tra sottosistemi di infrastruttura (webserver, long run process server, dbms server, NAS) o applicativi (comunicazioni da/verso sistemi ministeriali e/o di terze parti mediante identificazione degli enti coinvolti nello scambio dei flussi informativi e degli utenti abilitati all'accesso ai servizi anche tramite l'utilizzo di

certificati digitali).

I servizi sono sottoposti a controllo costante dell'erogazione e delle prestazioni del servizio mediante strumenti di supervisione, accessibili via web dal personale abilitato.

Di seguito le caratteristiche del gestionale espresse in forma sintetica che saranno dettagliate nei paragrafi successivi.

a. Erogazione servizio tramite protocollo https
b. Accessi al software protetti da "nome utente" e "password".
c. password di accesso "sicure".
d. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.
e. Protezione dei dati
f. Tracciabilità dei log di accesso per eventuali comunicazioni di Data Breach.
g. Tracciabilità delle variazioni ai dati del sistema

Erogazione servizi mediante protocollo HTTPS

Sia i servizi di backoffice che i servizi on line di Urbi Smart 2020 possono essere erogati mediante protocollo HTTPS. Il protocollo HTTPS consiste nel far transitare la comunicazione tramite il protocollo HTTP all'interno di una connessione criptata dal Transport Layer Security (TLS)/Secure Sockets Layer (SSL). Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti. Il principio che sta alla base di HTTPS è quello di avere:

- un'autenticazione del sito web visitato
- protezione della privacy
- integrità dei dati scambiati tra le parti comunicanti.

Accessi al software protetti da nome utente e password

Il **SPIGD** utilizza un sistema di **autenticazione basato su sessione** che verifica la validità della sessione in corso (identificata da un token di sessione) prima di fornire la pagina richiesta.

Allorchè la sessione sia scaduta o non sia attiva, qualsiasi richiesta viene ridirezionata al sistema di autenticazione. Il sistema di autenticazione standard prevede autenticazione basata su **Login e Password**; L'utente è identificato all'interno di una base dati da un *nome utente* e da una *password*, secondo lo schema seguente:

- login: nomeutente@identificativodb
- password: Password_Utente

Nomeutente, identificativodb e password sono gli elementi essenziali e univoci per procedere alla validazione di un utente.

Password di accesso sicure

Le password sono tutte crittografate mediante una implementazione derivata dello standard AES (Advanced Encryption Standard) a 256bit. Ad ogni utente, l'Amministratore applicativo può assegnare:

1. **Data Scadenza Utente**: questa data indica la data fino alla quale l'utente è valido. **Scaduta questa data l'utente viene disattivato**. Questa data serve per consentire di attivare un utente per un certo periodo di tempo: se si lascia il campo vuoto, oppure impostato a valore infinito 31-12-9999, l'utente è sempre attivo.
2. **Password d'Ufficio**: se non diversamente specificato, l'utente è costretto a modificare la password la prima volta che entra nella procedura.
3. **Data Attivazione Password:** questa data (impostata di default al giorno di creazione dell'utente) indica la data di attivazione della password per l'utente. In alcuni casi può essere utile attivare gli utenti in date posteriori alla creazione dell'utente stesso.
4. **Giorni Validità Password:** indica per quanti giorni la password di un utente è valida, a partire dalla data di attivazione. Questo campo è utile per definire un periodo di validità della password all'interno del range definito tra la data attivazione e la data scadenza. L'Amministratore applicativo può decidere la policy utente alla scadenza dei giorni di validità. Le due scelte possibili sono: a) Costringere l'utente a cambiare password

b) disattivare l'utente

5. **Max Giorni Non Loggato:** indica il numero massimo di giorni in cui un utente può restare attivo senza accedere al **SPIGD**. Trascorso tale numero di giorni senza che l'utente acceda al sistema, la procedura lo disattiva in automatico.

All'atto della creazione di un nuovo utente, l'Amministratore gli attribuisce:

1. la **Password** (di default viene impostata come password d'ufficio)
2. la **Data di Scadenza Utente**
3. la **Data di Attivazione della Password** (impostata alla data del giorno) e il numero di **Giorni di Validità della Password**
4. il numero **Max Giorni Non Loggato** (se si vuole che venga disattivato l'utente che non accede al **SPIGD**

per più di un certo numero di giorni consecutivi).

La prima volta che il nuovo utente entra nella procedura deve utilizzare la password attribuita dall'amministratore. Se la password assegnatagli è una **password d'ufficio**, il sistema gli presenta in automatico la sezione per il cambio password obbligatorio: **l'utente deve inserire una nuova password compresa tra 8 e 30 caratteri (almeno 2 numeri e almeno 5 lettere dell'alfabeto ed almeno un carattere tra . ; $! - < >)**. Modificata la password può ritornare al **SPIGD** tramite link contenuto nella maschera. Se l'utente sbaglia le credenziali per tre volte consecutive viene disabilitato, e può essere riabilitato solo mediante l'intervento dell'Amministratore, che agirà sempre attraverso l'interfaccia di gestione utenti. Il numero minimo di tentativi disponibili per tentare l'accesso è settato a 3, ma l'Amministratore applicativo può decidere di aumentare questo valore, secondo le politiche interne al cliente.

Un utente viene inoltre disabilitato se:

1. è scaduto (**Data Scadenza Utente** scaduta)
2. è stato per **MaxGiorniNonLoggato** senza accedere a Urbi Smart 2020 (se tale valore è stato settato).
3. la sua password è scaduta (**Giorni Validità Password**, settato) ed è stato definito che alla scadenza l'utente debba essere disattivato.

Anche in questi casi è necessario riabilitarlo tramite l'intervento dell'Amministratore, come sopra. L'**annullamento** di un utente prevede di annullare logicamente l'utente medesimo, in modo da garantire che le credenziali di autenticazione non saranno mai più utilizzate per diversi utenti, neppure in tempi diversi. Un utente **ANNULLATO** viene ancora visualizzato nella lista degli utenti, ma non è più attivo e non è più possibile effettuare operazioni su di esso. In questo modo si garantisce che non sarà mai inserito un utente con lo stesso nome di un utente già utilizzato in precedenza (anche se annullato).

Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.

Il **SPIGD** permette la definizione di tre tipologie di utenti in funzione della loro visibilità ed accessibilità alle varie procedure, e quindi in funzione del tipo di menù assegnato. In particolare:

1. **Utente Standard**: l'utente può entrare nell'area delle procedure abilitate ed accedere di default a tutti i programmi raggiungibili in virtù del suo Profilo Primario (Visione, Gestione, Supervisore). È tuttavia possibile prevedere un ulteriore livello di autorizzazione, disabilitando l'accesso solo ad alcuni programmi.
2. **Utente Scrivania**: questo tipo di utente può accedere esclusivamente ai programmi che gli sono stati espressamente abilitati. L'utente Scrivania può accedere solamente alle procedure che gli sono state assegnate, e la pagina di accesso proposta contiene soltanto i programmi che gli sono stati assegnati (non ha la navigazione completa dell'utente Standard).
3. **Utente Misto**: è l'utente che è Standard per alcune procedure e Scrivania per altre. Ad esempio: un utente standard dell'anagrafe (che ha a disposizione tutte le scelte del menù anagrafico) al quale viene attivata la sola funzione di visualizzazione delle delibere o

visualizzazione dei protocolli.

Protezione dei dati

Anche per la protezione dell'accesso ai dati, il meccanismo si fonda su un sistema di permessi basato sui ruoli definiti in pianta organica e nella gestione utenti descritta al paragrafo precedente. L'accesso ai dati avviene solo attraverso l'applicazione; i server di database sono protetti **da un doppio sistema di firewall e da regole di routing** che non ne consentono la visibilità dall'esterno della rete.

La gestione della base dati unica relativa al singolo Ente è basata su database standard. Nel caso di utilizzo del sistema in modalità Cloud con collegamento al Data Center, il database adottato è Maria DB. In tutti i casi il sistema ne rispecchia le caratteristiche in termini tecnico-funzionali.

Tracciabilità dei log di accesso (per eventuali comunicazioni di Data Breach)

Il sistema di autenticazione basato su sessione rende implicitamente disponibile una funzione di monitoraggio attività sul sistema. Attraverso apposita tabella, infatti, possono essere memorizzate le sessioni d'uso istanziate e chiuse, i tentativi di accesso non riusciti, i rinnovi di sessione, ecc. La richiesta al Session Manager, inoltrata ogni qualvolta un utente fa una richiesta al **SPIGD**, consente di registrare informazioni sulle operazioni fatte con tracciamento per ogni utente, programma, evento. La logica di base con cui sono sviluppati i programmi nel **SPIGD** fa sì che ciascuna operazione fatta dagli utenti (visualizzazione di una maschera, inserimento, modifica o rimozione di dati) avvenga tramite il richiamo di un evento che viene tracciato. Vengono difatti tracciati:

- token di sessione
- utente loggato
- Remote IP da cui è pervenuta la chiamata
- TimeStamp dell'evento
- estremi della chiamata

La struttura è in grado di memorizzare anche situazioni del tipo:

- "Non si dispone delle credenziali per procedere." @ErroreLogin (dove ErroreLogin riporta l'esatta motivazione dell'errore)
- "Errore in fase di derivazione delle credenziali per la base dati. Chiudere e riaprire il browser, quindi riprovare"
- "Sessione non valida!"
- "Sessione scaduta!"
- "Sessione con IP reimpostato, rieffettuare la login!"
- "Non si dispone delle autorizzazioni per accedere, chiudere il browser e rieffettuare la login!"
- LOGIN utente
- LOGOUT Utente.

Tracciabilità delle variazioni ai dati del sistema

Il **SPIGD** è dotato di un sistema di monitoraggio delle variazioni alla base dati. Le variazioni applicative alla base dati vengono tracciate riportando, per ogni sessione di variazione:

- grandezza variata
- utente che ha effettuato la variazione
- istanza applicativa che ha provocato la variazione
- valore precedente alla variazione
- valore successivo alla variazione.

Funzioni applicative di interrogazione consentono l'analisi del monitoraggio.

Erogazione servizio di assistenza remota

Il **SPIGD** è dotato di un servizio di assistenza remota, attraverso uno specifico settore di Help Desk e mediante due modalità differenti:

1. collegamento da remoto mediante software di accesso a desktop remoto, incluso nel

contratto di assistenza;

2. accesso da remoto, tramite l'utente "PAD_SUPPORT", adottato solo a seguito di sottoscrizione da parte del cliente di una specifica autorizzazione formale.

Collegamento da remoto

Viene utilizzata questa modalità nei casi in cui l'Operatore di Help Desk, per erogare il supporto al cliente richiedente, non abbia la necessità di operare sul sistema del cliente ma solamente di guidare l'Utente e visualizzare le operazioni che quest'ultimo effettua sull'applicativo.

Il collegamento viene effettuato mediante un software di accesso a desktop remoto, leader di mercato, che garantisce la sicurezza degli utenti e delle connessioni mediante infrastruttura certificata ISO/IEC 27001 e interamente conforme alle norme HIPAA e SOC2:

- Crittografia AES a 256 bit
- Autenticazione a due fattori
- Protezione da forza bruta
- Lista bianca per utenti e IP
- Elenco dei dispositivi fidati
- Reset della password forzato.

Accesso mediante utente "PAD_SUPPORT"

A seguito dell'autorizzazione del cliente, predisposta su carta intestata, debitamente sottoscritta e trasmessa via PEC viene creato uno specifico utente e provvede alla configurazione dell'ambiente di lavoro.

Per mezzo di questa modalità gli Operatori di Help Desk possono accedere in autonomia al database del cliente tramite uno specifico utente di sistema creato ad hoc (PAD_SUPPORT), al fine di risolvere direttamente, dove possibile, le problematiche segnalate, senza la necessità che una persona che presidi l'intervento. Attraverso questa modalità si incrementa l'efficienza dei servizi di Assistenza, velocizzando i tempi di risposta e procedendo in maniera più rapida alla risoluzione delle problematiche evidenziate, nel rispetto della trasparenza così come della normativa sulla privacy, attraverso una puntuale tracciatura delle attività effettuate dagli Operatori di Help Desk. Tutte le operazioni sono infatti tracciate in uno specifico log che, al termine dell'intervento, viene firmato digitalmente, marcato temporalmente, allegato al ticket di assistenza e messo in conservazione digitale e messo a disposizione del cliente nel caso in cui lo richieda.

Nell'eventualità che, per una specifica richiesta d'assistenza, il cliente non voglia permettere l'utilizzo di tale funzionalità, in fase di inserimento del ticket, il richiedente deve disabilitare il check "Assistenza tramite Backdoor", che di base è sempre valorizzato.

Subappalto di servizi

Nei casi in cui la ditta che eroga il **SPIGD** abbia la necessità di subappaltare una componente e/o alcune attività previste dal servizio in modalità Cloud, dopo aver verificato i requisiti di esperienza, di professionalità, di capacità e di affidabilità del fornitore, sottoscrive con quest'ultimo un contratto formale che contiene, oltre alle clausole contrattuali, il disciplinare tecnico che regolamenta la modalità di erogazione del servizio da prestare e le misure di sicurezza da adottare per garantire la sicurezza delle informazioni e di tutti i dati trattati (con particolare riguardo verso le Informazioni Personali Identificabili - PII).

Nel caso in cui il fornitore, per espletare il proprio servizio, non sia tenuto ad effettuare alcun trattamento di dati personali, tale divieto è espressamente indicato nel contratto di servizio.

Nel caso in cui il fornitore debba effettuare un trattamento di dati personali, tale fornitore, per ogni servizio assegnato, viene nominato Sub-Responsabile del trattamento dei dati in

outsourcing, e nella lettera di nomina sono riportate:
- le finalità del trattamento
- i dati da trattare
- la base giuridica
- la durata del trattamento
- le indicazioni nonché le specifiche istruzioni a cui attenersi affinché tutte le operazioni di trattamento informatico e manuale dei dati personali, nei limiti delle competenze e attribuzioni del fornitore, siano effettuate nel rispetto della normativa vigente e dei regolamenti aziendali in materia di tutela dei dati personali, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento UE 679/16 (art. 28 comma 4).