ISTITUTO COMPRENSIVO

"DON L. MILANI"

Caltanissetta

Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi

(MdG)

Via Filippo Turati s.n. – Caltanissetta (CL)

Codice Meccanografico CLIC830004 Codice Fiscale 92062090854

Tel 0934 598587 – Fax 0934 598008

clic830004@istruzione.it clic830004@pec.istruzione.it

Indice

1. PRINCIPI GENERALI

1.1. PREMESSA

Il decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica del 20 ottobre 1998[1] n. 428", all'art. 3, comma 1, lettera c), prevede per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del Manuale di gestione.

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio". In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DsPR n. 428 del 20 ottobre 1998 [1]).

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

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

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

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

Esso disciplina:

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto al protocollo informatico;

[1] *Il DPR del 20/10/1998 n. 428 è stato abrogato nel DPR del 20 dicembre 2000, n. 445.*

- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del titolario di classificazione e del massimario di selezione e di scarto;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

1.2. AMBITO DI APPLICAZIONE DEL MANUALE

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 5, comma 1) del decreto del Presidente del Consiglio dei Ministri 3 Dicembre 2013, recante le regole tecniche per il protocollo informatico, e successive modifiche ed integrazioni normative.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'ISTITUTO COMPRENSIVO "DON L. MILANI" Caltanissetta a partire dal 30/11/2015.

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa. Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3.DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:

- per "amministrazione", l' dell'ISTITUTO COMPRENSIVO "DON L. MILANI" Caltanissetta;
- per "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per Regole tecniche, il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428; IL DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 DICEMBRE 2013; IL DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 novembre 2014; Circolare 23 gennaio 2013 n.60 dell'Agenzia per l'Italia Digitale;
- per Codice, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale.

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

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **PdP** - Prodotto di Protocollo informatico – l'applicativo in uso all'amministrazione; di fatto è il sistema di gestione documentale inteso come Sistema Software utilizzato dall'Amministrazione che permette di gestire il sistema di gestione del protocollo informatico e gestione documentale e degli archivi.
- **AOO** Area Organizzativa Omogenea;
- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.
- **ARCHIVIAZIONE:** è il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. E' passo propedeutico alla conservazione e per il quale non sono previsti particolari obblighi di legge.
- **CNIPA:** Centro Nazionale per l'Informatica nella Pubblica Amministrazione. DigitPA : Ente Nazionale per la Digitalizzazione della Pubblica Amministrazione AID: Agenzia per l'Italia Digitale
- **CONSERVAZIONE:** il processo che consente di conservare i documenti in moda-lità informatica a norma di legge e che risponde a quanto stabilito nella delibera- zione Cnipa 11 del 19 febbraio 2004.
- **CONSERVAZIONE SOSTITUTIVA**: vedi conservazione
- **DOCUMENTO ANALOGICO ORIGINALE:** documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

- **DOCUMENTO INFORMATICO:** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- **EVIDENZA INFORMATICA:** una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1 comma 1 lettera r deliberazione CNIPA 11 del 19 febbraio 2004).
- **FATTURAZIONE ELETTRONICA:** il processo che risponde a quanto richiesto dal decreto del 23 gennaio 2004 del Ministero dell'Economia e delle Finanze e dal decreto Legislativo 20 febbraio 2004 n. 52.
- **FIRMA ELETTRONICA:** come "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"; così come definita all'art. 1 comma 1 lettera t Decreto Legislativo del 7 marzo 2005 n. 82 e successive modificazioni.
- **FIRMA DIGITALE:** come "Un particolare tipo di firma elettronica qualificata basata 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".
- **FIRMA ELETTRONICA QUALIFICATA:** come "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica"
- **FIRMA ELETTRONICA AVANZATA:** come insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
- **IMPRONTA (o HASH):** la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art. 1 comma 1 lettera s deliberazione CNIPA 11 del 19 febbraio 2004).
- **LOTTO DI ARCHIVIAZIONE:** insieme di documenti raggruppati secondo un criterio di aggregazione, aventi un file indice (file di chiusura del lotto) che

attesta la conservazione con l'apposizione della firma del responsabile della conservazione e della marca temporale.

- **MARCA TEMPORALE:** così come definita all'art. 1 comma 1 lettera i DPCM del 13 gennaio 2004.
- **PDF:** Portable Document Format. E' un formato di file che cattura, in formato elettronico, tutti gli elementi di un documento stampato in modo che sia possibile visualizzarli, stamparli e scambiarli fra più utenti. E' un formato proprietario di Adobe e per creare file PDF sono necessari Adobe Acrobat, Adobe Capture o prodotti simili. Viceversa per visualizzare un file PDF è necessario Adobe Acrobat Reader disponibile gratuitamente.
- **RESPONSABILE DELLA CONSERVAZIONE** (RdC): vedi responsabile del procedimento di conservazione sostitutiva.
- **RESPONSABILE DEL PROCEDIMENTO DI CONSERVAZIONE SOSTITUTIVA:** il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva conformemente a quanto previsto all'art. 5 della deliberazione Cnipa 11 del 19 febbraio 2004.
- **RIFERIMENTO TEMPORALE:** informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
- **XML:** Extensible Markup Language. Linguaggio derivato dall'SGML (Standard Generalized Markup Language) il metalinguaggio, che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la de- scrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire libera- mente anche gli attributi dei singoli marcatori.

Per le Norme ed i Regolamenti di riferimento vedasi l'elenco riportato nell'allegato 1 "-NORMATIVA DI RIFERIMENTO-".

1.4. AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata **AOO-CLIC830004** che è composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato nell'allegato 2 "-AOO-".

All'interno della AOO il sistema di protocollazione è unico.

Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme degli UOR che la compongono con la loro articolazione in UU.

All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, mentre è decentralizzato, per la corrispondenza in uscita, attraverso tutte le UOR che svolgono anche i compiti di UOP.

L'allegato 2 "-AOO-" è suscettibile di modifica in caso di inserimento di nuove (AOO/)UOP/UOR/UU o di riorganizzazione delle medesime.

Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali.

L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UOR allo svolgimento dell'attività di protocollazione.

Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del responsabile del protocollo informatico.

Nelle UOR sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

1.5. SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO

Nell' AOO è istituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).

Egli è funzionalmente individuato nel UOP - Ufficio di Protocollo.

1.6. FIRMA DIGITALE

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

Nell'allegato 3 "-Firma Digitale-" viene riportato l'elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione.

1.7. TUTELA DEI DATI PERSONALI

L'amministrazione titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.

Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 3.

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

- al principio di necessità nel trattamento dei dati;
- al diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

1.8. CASELLE DI POSTA ELETTRONICA

L'AOO è dotata di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza in ingresso: CLIC830004@pec.istruzione.it, si è altresì dotata di una casella di Posta Elettronica Certificata per la corrispondenza in entrate e in uscita: segreteria@pec.istitutocomprensivodonlmilani.gov.it direttamente collegata al PdP, pubblicate sull'Indice delle Pubbliche Amministrazioni (IPA).

Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.

L'AOO è dotata anche di una caselle di posta elettronica ordinaria per la corrispondenza in ingresso: CLIC830004@istruzione.it e di una casella di posta

elettronica ordinaria per la corrispondenza in entrata ed in uscita: segreteria@istitutocomprensivodonlmilani.gov.it direttamente collegata al PdP.

Inoltre l'AOO si è dotata di più caselle di posta elettronica ordinaria interne, di servizio, una per ogni Ufficio Utente / operatore, destinata a raccogliere tutti messaggi di posta elettronica di servizio per la gestione delle comunicazioni generate dal PdP.

1.9. SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI

Con l'inizio dell'attività operativa del protocollo unico viene adottato un unico titolario di classificazione per l'archivio centrale unico (logico) dell'amministrazione.

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

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico.

1.10. TITOLARIO O PIANO DI CLASSIFICAZIONE

1.10.1. TITOLARIO

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc.

Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo dell'amministrazione.

Il titolario è uno strumento suscettibile di aggiornamento.

L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP (oppure, su proposta del

responsabile dell'archivio generale dell'amministrazione e/o dalle autorità competenti per materia).

La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno.

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

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

Per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione.

Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo titolario e valgono almeno per l'intero anno.

Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

1.10.2. CLASSIFICAZIONE DEI DOCUMENTI

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse, etc.), *opzionale -il numero del fascicolo ed eventualmente del sottofascicolo* -.

1.11. FORMAZIONE

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro della funzione pubblica sulla formazione e la valorizzazione del personale

delle pubbliche amministrazioni, l'amministrazione ha stabilito percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

In particolare, considerato che il personale assegnato agli UOP deve conoscere sia l'organizzazione ed i compiti svolti da ciascun UOR/UU all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, sono stati previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

- ai processi di semplificazione ed alle innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti della AOO;
- agli strumenti e alle tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione/AOO;
- alle norme sulla protezione dei dati personali e alle direttive impartite dal presente manuale nel Capitolo "3. PIANO DI SICUREZZA" e con il documento programmatico della sicurezza.

Tenute presenti le disponibilità di bilancio, in relazione anche al combinato disposto dell'art. 2 del CCNL 31 marzo 1999 e dell'art. 4 del CCNL 1 aprile 1999, nella impossibilità di organizzare autonomi corsi, è favorita l'adesione a corsi di formazione gratuiti organizzati, per il personale dei servizi informatici e per quello impegnato nelle attività di registrazione del protocollo, dalle amministrazioni centrali o territoriali.

1.12. ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA

L'amministrazione/AOO si è dotata di più caselle di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; l'UOP medesima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico dal CNIPA fornendo le seguenti informazioni che individuano l'amministrazione stessa IN UN'UNICA AOO.

Le informazioni inerenti all'amministrazione sono riportate nell'allegato 2 "-AOO-". Il codice identificativo della amministrazione associato alla propria AOO, è stato generato e attribuito autonomamente dall'amministrazione.

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

tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione ovvero la creazione di una AOO.

1.13. PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dalla deliberazione CNIPA n. 11/2004. Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunica al CNIPA le procedure integrative che intende adottare ai sensi dell'art. 7 della citata deliberazione.

2. ELIMINAZIONE DEI PROTOCOLLO DIVERSI DAL PROTOCOLLO INFORMATICO

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico.

2.1. PIANO DI ATTUAZIONE

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono registrati all'interno del registro di protocollo informatico.
Per i documenti interni, quali Circolari, Contratti e Decreti si ritiene opportuno gestire il progressivo di registrazione separato dal registro di protocollo.

3. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate all'interno dell'Amministrazione per l'accesso ai sistemi informatici, per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

3.1. OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

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

3.2. GENERALITÀ

Il RSP ha predisposto il piano di sicurezza in collaborazione con Attori interni: il responsabile del sistema informativo ed il responsabile del trattamento dei dati personali e, Attori Esterni: Società Gestore del PdP *e* Consulenti Informatici Incaricati.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

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

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.

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

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno 60 giorni durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura del UOP-Ufficio di Protocollo delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica ricorrendo a strutture esterne qualificate;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

3.3.POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

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

È compito del RSP, assistito dalla società fornitrice del PdP o consulente esterno procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.

Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di audit.

In ogni caso, tale attività è svolta almeno con cadenza annuale.

3.4.POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO

3.4.1.Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.
2. Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.
3. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

3.4.2.Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.
2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
3. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

3.4.3.Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ecc)
2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione "affittate" da questa.

3.4.4.Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo devono essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
3. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
4. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

3.4.5.Politiche - Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione deve porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

1. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad

utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password devono essere cambiate con il primo accesso al sistema informativo e successivamente, ogni 60 giorni, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a 30 giorni.

3. Tutte le postazioni di lavoro (PC da tavolo e portatili) devono essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "newsgroup" che utilizzano il sistema di posta elettronica dell'Amministrazione devono contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, sono dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.
8. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.
9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

3.5. POLITICHE - USO NON ACCETTABILE

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.5.1.Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
10. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
    b. attività di "sniffing";
    c. disturbo della trasmissione;
    d. spoofing dei pacchetti;
    e. negazione del servizio;
    f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;

g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

11. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
12. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
13. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
14. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
15. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.5.2. Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

3.6. POLITICHE - ANTIVIRUS

3.6.1.Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri

sistemi con conseguenza negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

3.6.2.Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

3.6.3.Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

3.6.4.Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (CD, DVD, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet utilizzando ad esempio sistemi di connessione mobile.

- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.
- Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.
- Non utilizzare i server di rete come stazioni di lavoro.
- Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.
- Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.
- Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.
- Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.
- Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
- È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

3.6.5.Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti; diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

3.7. POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

3.7.1.Scopo

Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

3.7.2. Ambito di applicazione

Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

3.7.3. Politiche

Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.

Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario

3.8. POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

3.8.1.Scopo

Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

3.8.2.Ambito di applicazione

La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

3.8.3.Politiche – Usi proibiti

Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

3.8.4.Politiche – Uso personale

Non è ammesso l'uso della posta istituzionale per usi personali.

3.9.POLITICHE PER LE COMUNICAZIONI WIRELESS

3.9.1.Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

3.9.2. Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.
2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

3.9.3. Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing).
3. Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

3.9.4. Politiche – Approvazione delle tecnologie

Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

3.10. FORMAZIONE DEI DOCUMENTI – ASPETTI DI SICUREZZA

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

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

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

I documenti informatici prodotti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard

(PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

3.11. GESTIONE DEI DOCUMENTI INFORMATICI

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

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

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.11.1. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.

Nella conduzione del sistema informativo l'amministrazione ha predisposto specifiche istruzioni per l'utilizzo dei sistemi hardware e software in relazione alla sicurezza informatica. In particolare, in considerazione che le soluzioni informatiche per la gestione Documentale sono accessibili attraverso la rete internet, si è provveduto a formare in maniera specifica sui possibili pericoli provenienti da Internet. Si sono approfonditi i temi riguardanti lo SPAM, il PHISHING, i VIRUS, i WORM, ecc.. Descrivendo gli aspetti relativi alla sicurezza informatica basandoli su un approccio orientato ai servizi secondo un modello strutturato del tipo Causa – Effetto – Soluzione. Quindi per ogni servizio utilizzato nell'ambito della gestione documentale sono state riportate le possibili vulnerabilità, gli attacchi possibili, gli effetti che questi producono e le soluzioni per difendersi.

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, non sono state individuate funzioni specifiche ma è stata adottata una soluzione distribuita su tutti gli Uffici Utente :

In relazione alla componente fisica della sicurezza non sono stati definiti ruoli interni ma l'amministrazione si avvale di esperti esterni.

3.11.2. COMPONENTE FISICA DELLA SICUREZZA

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- L'accesso fisico è garantito/protetto dall'utilizzo di porte di sicurezza, da personale di custodia durante le ore di apertura e da sistema di allarme durante le ore di chiusura.

Le misure di sicurezza fisica hanno un'architettura multi livello:

- A livello di Servizio di utilizzo del PdP e archiviazione corrente nonchè di gestione del Servizio di BackUp l'onere della sicurezza fisica è a carico della società gestore

- a livello di sede dell'amministrazione/AOO che ospita il sistema di conservazione sostitutiva, le unità di archiviazione sono collocate in locale non accessibile al personale non autorizzato e protetto da porta di sicurezza;
- a livello di sede dell'amministrazione/AOO e di locale/i che ospita/no le risorse elaborative e di trasmissione del sistema informatico è inibito l'accesso a personale non autorizzato. Non sono in atto altre misure fisiche al di fuori di quelle sopra indicate.

3.11.3. COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del PdP, è stata realizzata attraverso:

- *utilizzo di Posta Elettronica Certificata*
- *utilizzo di firme digitali*
- *utilizzo di trasmissioni attraverso sistemi di codifica con certificato digitale*

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura Proxy/Firewall

3.11.4. COMPONENTE INFRASTRUTTURALE DELLA SICUREZZA

Il sistema informatico interno utilizza un impianto Proxy/Firewall per il collegamento alla rete internet.

3.11.5. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA

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

Le registrazioni di sicurezza sono costituite:

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

Le registrazioni di sicurezza sono soggette alle misure illustrate nei precedenti paragrafi.

3.12. TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'amministrazione oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

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

3.12.1. ALL'ESTERNO DELLA AOO (INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO)

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

e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

3.12.2. ALL'INTERNO DELLA AOO

Gli Uffici dell'amministrazione (UOP/UOR) si scambiano documenti informatici attraverso l'utilizzo prioritario del sistema di WorkFlow offerta dal PdP o in alternativa con le caselle di posta elettronica di servizio assegnata a ciascuna UU in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l' "impiego della posta elettronica nelle pubbliche amministrazioni".

3.13. ACCESSO AI DOCUMENTI INFORMATICI

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

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

Queste, in sintesi, sono:

- lettura,
- inserimento,
- modifica,
- annullamento;

In particolare ogni Operatore/UU viene profilato sul PdP in uso secondo il seguente schema (ACL) *Access control list* - lista di controllo degli accessi:

- abilitazione alle procedure/applicazioni che può utilizzare,
- abilitazione ai singoli campi dei record di registrazione che può gestire,
- abilitazione singoli record di registrazione documentale;

Le regole per la composizione delle password e per il blocco delle utenze prevedono il controllo della composizione della password verificando il corretto rispetto delle regole imposte (minimo 8 caratteri, minimo 1 lettera maiuscola, 1 minuscola, 1 numero e 1 carattere speciale). Il Blocco utente avviene al terzo tentativo errato.,

In abbinamento alla digitazione del nome utente e password è stato inserita l'interazione con un sistema captcha ("***c****ompletely* ***a****utomated* ***p****ublic* ***T****uring test to tell* ***c****omputers and* ***h****umans* ***a****part*" - Test di Turing pubblico e completamente automatico per distinguere computer e umani).

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Quindi, il PdP adottato dall'amministrazione/AOO:

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

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

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

3.13.1. UTENTI INTERNI ALLA AOO

I livelli di autorizzazione per l'accesso alle funzioni del PdP sono attribuiti dal RSP dell'amministrazione/AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione/annullamento e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti criteri operativi:

Classe Utenti Interni

Ruolo	**Descrizione**
Amministratore	Categoria Sono gli Amministratori del PDP adottato. Forniscono il supporto delle attività previste dalla gestione dei servizi.

	Esigenza primaria Garantire il Controllo dei servizi erogati (Erogazione e accesso all'Informazione). Attività principale Attività operative connesse alle funzioni di gestione. Gli Amministratori si occupano della creazione e gestione degli utenti; della Definizione e dell'organizzazione (architettura informativa) dei contenuti informativi; gestire il processo di revisione, approvazione e pubblicazione dei contenuti.
	Ambito operativo Area riservata (funzioni operative dedicate).
Utente Interno (UU, Operatore, Redattore, o *content- publisher e Archivisti*)	Categoria Sono operatori, con diritti di gestione dei documenti e pubblicazione sui contenuti informativi che integrano i servizi transazionali; appartengono alla struttura organizzativa dell'Ente. Esigenza primaria Garantire adeguati livelli di qualità (completezza, aggiornamento, coerenza) di contenuti informativi e documenti. Attività principale Gestione del sistema documentale e dei contenuti informativi. Ambito operativo Area riservata (funzioni operative dedicate)

Gruppo Utente (UOP)	Categoria Sono gruppi di operatori, con diritti di gestione dei documenti e pubblicazione sui contenuti informativi che integrano i servizi transazionali; appartengono alla struttura organizzativa dell'Ente. Esigenza primaria Garantire adeguati livelli di qualità (completezza, aggiornamento, coerenza) di contenuti informativi e documenti. Attività principale Gestione del sistema documentale e dei contenuti informativi. Ambito operativo Area riservata (funzioni operative dedicate)

Per soddisfare le esigenze di tutte queste categorie di utenti, la soluzione offre un insieme di caratteristiche che, secondo una strutturazione in livelli, possiamo classificare come:

funzionali, ossia di servizi e funzionalità disponibili per le diverse categorie di utenti, secondo il ruolo di ciascuno nel sistema;

applicative, ossia di componenti e moduli software che implementano i servizi e le funzionalità citati in termini di gestione dell'interfaccia utente, dei contenuti, della sicurezza, ecc..

3.13.2. ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO

Gli utenti abilitati accedono al PdP attraverso una pagina unica di autenticazione/LogIn.

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.

Il "file delle password" utilizzato dal servizio di accesso è una struttura crittografata e accessibile soltanto da un processo di sistema.

Tutte le utenze dell'AOO sono configurate con un time-out che provvede a disconnettere automaticamente l'applicazione dopo 30 minuti di inattività.

Le sessioni multiple con la stessa user ID sono proibite e impedite dal PdP.

3.13.3. MODALITÀ DI CREAZIONE E GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO

Le utenze sono create dall'utente amministratore del PdP.

In caso di smarrimento della password solo l'utente amministratore del PdP può procedere al suo ripristino.

3.13.4. CONSULTAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO PARTICOLARI

Il complesso dei documenti per i quali è stata attivata la registrazione di protocollo particolare costituisce l'archivio particolare.

I documenti e i fascicoli dell'archivio particolare sono consultabili nel rispetto delle seguenti norme:

- art. 24 della legge 7 agosto 1990, n. 241, e successive modificazioni;
- art. 8 del decreto del Presidente della Repubblica 27 giugno 1992, n. 352;
- artt. 107 e 108 del decreto legislativo 29 ottobre 1999, n. 490.

3.13.5. ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- Gestione Utenti
- Gestione Gruppi Utenti

La visibilità completa (o parziale) sul registro di protocollo è consentita **gruppo di utenti** abilitati.

L'utente assegnatario dei documenti protocollati è invece abilitato a consultare e modificare (solo fase di produzione documentale) il documento assegnato.

L'operatore che gestisce lo smistamento dei documenti può assegnare secondo specifiche regole di WorkFlow documentale.

Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa sul documento stesso è possibile solo agli utenti assegnati al gruppo di condivisione particolare definito con il gruppo di condivisione "196"

3.13.6. UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI

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

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

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

3.13.7. UTENTI ESTERNI ALLA AOO - PRIVATI

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP).

L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente attraverso il sistema di autenticazione in uso all'AOO e offerto dal PDP in Uso.

L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il PdP sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.

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

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

Agli utenti esterni riconosciuti ed abilitati alla consultazione dei dati propri presenti all'interno dell'amministrazione sono fornite tutte le informazioni necessarie per accedere a detti documenti amministrativi.

Per l'accesso per via telematica è possibile identificare le tipologie e i ruoli previsti:

Classe Utenti Esterni	
Tipologia	**Descrizione**
Utente non registrato (anonimo)	Categoria Chiunque accede al sistema tramite Internet; si tratta di soggetti che richiedo alle sezioni Pubbliche del Portale informazioni generiche (ad esempio sfogliare le sezioni di amministrazione trasparente e accedere alle pubblicazioni dell'Albo). Esigenza primaria Qualità e fruibilità dell'informazione: informazioni corrette, complete e aggiornate rese fruibili attraverso strumenti, di semplice utilizzo, in grado di consentire forme efficaci di accesso all'informazione. Attività (modalità d'interazione) L'Utente è passivo rispetto alle informazioni ricevute; fanno parte di questa categoria tutti i servizi d'informativa, rivolti di volta in volta a tutti indistintamente (**informativa generale**) o a specifici gruppi di interesse (**informativa specialistica**). Modello di comunicazione *standard* Ambito operativo Area pubblica (funzioni operative non dedicate).
Utente registrato / riconosciuto (*)	Esigenza primaria Informazioni selezionate, comunicazioni, circolari, documenti richiesti, ecc.

	Attività (modalità d'interazione) L'Utente è attivo nel caso in cui esista uno scambio d'informazioni tra l'utente ed il soggetto erogatore di servizi; in questo caso l'utente si configura come una componente attiva del processo di comunicazione (**informativa individuale** e **servizi**). Modello di comunicazione Personalizzato. Ambito operativo Area riservata (funzioni operative dedicate).

(*) L'utente esterno si definisce "riconosciuto" quando il processo di registrazione è integrato da procedure che consentono una forma d'identificazione dell'Utente stesso.

4. CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione dei documenti informatici avviene con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11.

4.1. SERVIZIO ARCHIVISTICO

Il responsabile del sistema archivistico dell'AOO si avvale per l'archiviazione dell'archivio corrente del PdP in uso che prevede la collocazione dei documenti e della Base Dati di gestione e classificazione nel sistema Cloud offerto dal sistema stesso.

I server che rendono disponibile il PdP sono collocati nel Data Center di Aruba S.p.A.. Lo stabile è sorvegliato da personale specializzato 24 ore al giorno; la sala CED, dove si trovano i dispositivi hardware e software dei diversi sistemi di servizio al PdP, la sala di controllo dell'alimentazione elettrica, del sistema idraulico, del condizionamento e la sala di monitoraggio dei sistemi di sicurezza installati, è accessibile solo mediante utilizzo di badge autorizzato ed è controllato da un sistema TVCC; le porte sono dotate d'allarmi; le stanze dell'area sono controllate mediante rivelatori combinati microonde e infrarossi. Le aree del CED sono dotate d'impianto di rilevazione fumi e antincendio.

Tutte le apparecchiature del centro dati sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso d'interruzione dell'erogazione dell'energia elettrica da parte del fornitore. In caso d'assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

Il centro dati è connesso alla rete internet con più dorsali fornite da diversi Carrier. In particolare i Server di servizio al PdP sono connessi con banda dedicata e garantita di 100 Mbit/sec.

Il Sistema di Servizio al PdP possiede due sistemi di gestione DNS collocati su reti diverse e quindi in grado di assicurare la massima continuità del servizio.

I sistemi sono inoltre connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne.

Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "default deny" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e

"defense in depth" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, ed infine a livello di sistema, hardening).
Quindi, il sistema ha le seguenti caratteristiche minime:

4.1.1.HOSTING E SERVIZI SISTEMISTICI

La piattaforma hardware prevede l'utilizzo di server collocati presso la Server Farm (sopra descritta) del PdP in uso con la seguente configurazione:

- Sistema Operativo di Tipologia Server idoneo,
- HTTPS / SSL Support,
- Hosting con Web Server, Applications Server, Data Base Server e BackUp Server su Hardware ad elevate capacità e prestazioni,
- Implementazione regole di firewalling su firewall: HTTP, HTTPS, ILS, POP3, SMTP, IDS,
- Manutenzione hardware
- Monitoraggio del server H24x7, con tracing di utilizzo di CPU e RAM, occupazione di spazio disco e corretto funzionamento delle componenti di rete
- Sistemi fisici anti intrusione,
- Gestione centralizzata del DNS
- Servizi di Posta elettronica con servizio web mail, antivirus ed antispam
- Servizi di Posta elettronica Certificata.

4.1.2.Gestione della Posta Elettronica

Tramite i **connettori per la posta elettronica** forniti dal PdP, la PEO (Posta Elettronica Ordinaria) e PEC (Posta Elettronica Certificata) Istituzionale viene protocollata ed archiviare direttamente nel sistema di archivio corrente.

4.1.3.BackUp Conservazione dei Dati

Sono previsti BackUp della base dati e dei File gestiti sui servizio Hosting dell'azienda fornitrice del PdP e BackUp del file di conservazione sostitutiva.
Per la gestione "**Data Base e Documenti Informatici dell'archivio Corrente**", il servizio di BackUp ha le seguenti policy:

1. BackUp Dati di tipo incrementale con frequenza settimanale
2. BackUp Dati di tipo Completo con frequenza mensile

Per la gestione di "Conservazione Sostitutiva" relativamente al **Pacchetto di Versamento generato dal sistema** (solo file indice e singoli documenti informatici), il servizio di BackUp ha le seguenti policy:

- BackUp Dati di tipo incrementale con frequenza settimanale

- BackUp Dati Applicativi di tipo Completo con frequenza mensile

Per la Conservazione Sostitutiva il servizio di backup ha la seguente Policy:

1. *BackUp Dati di tipo completo con frequenza settimanale.*

Infine il PdP è integrato di strumenti di BackUp attivabile direttamente dall'amministrazione/AOO. Quindi, il responsabile del servizio in argomento per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase per l'esecuzione di ulteriori copie di backup, con cadenza mensile, che includono le seguenti fasi:

1. Attivazione del servizio di generazione del Pacchetto di BackUp offerto dal dal PdP.
2. Trasferimento del Pacchetto di BackUp presso l'infrastruttura di archiviazione dell'Ente.

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

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

4.2. CONSERVAZIONE DEI DOCUMENTI INFORMATICI E DELLE REGISTRAZIONI DI PROTOCOLLO

Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

4.2.1. La conservazione sostitutiva dei documenti

La conservazione sostitutiva è il processo che presenta, e si avvale per la sua implementazione, di strumenti ed elementi diversi, regolati da discipline apposite che vanno raccordate alla disciplina generale della conservazione.

Per esemplificare può essere utile richiamare in sintesi gli strumenti/elementi principali:

1. ***Documento informatico***: è una realtà immateriale, il tipo di supporto fisico sul quale è registrato è irrilevante per la natura del documento stesso. Del documento informatico, a differenza di quello cartaceo, è possibile avere "n" esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano assicurate, in particolare, la sua integrità e autenticità. Esemplificando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
2. ***Documento analogico***: in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui, come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è solo quello cartaceo, ma può essere un film, una lastra o una pellicola radiologica, microfiche e microfilm, nastri audio e video. Il documento analogico può essere, originale, a sua volta distinto in originale unico e non unico, o copia.
3. ***Supporto di memorizzazione***: il supporto può essere ottico o non ottico poichè il documento esiste a prescindere dal supporto su cui è memorizzato. La deliberazione CNIPA 11/2004 autorizza l'utilizzo di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser, non solo quindi, dischi ottici WORM e CD-R, ma anche magneto-ottici e DVD. E' data, inoltre, la possibilità di utilizzare un qualsiasi altro supporto di memorizzazione, oltre a quelli a tecnologia laser, nel rispetto delle regole tecniche previste ed in mancanza di altri motivi ostativi. Si è, infatti, raggiunta la consapevolezza del fatto che gli strumenti di firma digitale e marca temporale garantiscono idoneamente l'integrità del documento nel processo di conservazione, indipendentemente dal supporto scelto. Sono gli stessi strumenti che garantiscono anche la possibilità di trasmissione telematica dei documenti senza che questo processo di trasmissione possa portare ad alte- razioni di sorta.
4. ***Firma digitale***: è l'elemento principale che interviene nella gestione elettronica del documento informatico a partire dalla formazione, trasmissione, fino alla conservazione, poiché conferisce al documento cui è

apposta piena vali- dità legale, assicurando autenticità, integrità, non ripudiabilità.

5. ***Attestazione temporale***: per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale" che è definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere questo risultato è la marca temporale, una particolare firma digitale che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

Il processo di conservazione ha il fine ultimo di trasformare un documento affinché diventi inalterabile e immodificabile e venga reso disponibile nel tempo nella propria autenticità ed integrità.

In linea generale non sono previste autorizzazioni preventive per l'adozione di criteri operativi per effettuare la conservazione sostitutiva.

Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali è però necessario rispettare le regole tecniche previste dalla normativa.

4.2.2.Il responsabile della conservazione

Il Responsabile della Conservazione di documenti in formato digitale assume insieme ai suoi delegati o ai terzi affidatari, un ruolo fondamentale all'interno del processo di conservazione sostitutiva ed è tenuto a gestire tale processo in modo da mantenerlo coerente con quanto stabilito dalla normativa in vigore. La presenza di tale figura è necessaria sia in ambito privato che pubblico con l'attribuzione di compiti, debitamente elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Uno degli obiettivi principali del responsabile della conservazione sostituiva è quello di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione sostituiva.

Più in particolare dovrà provvedere a:

1. definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conserva- re, tenendone evidenza;
2. organizzare conseguentemente il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche al fine consentire l'esibizione di ciascun documen- to conservato;

3. archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
   a. descrizione del contenuto dell'insieme dei documenti;
   b. estremi identificativi del responsabile della conservazione;
   c. estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
   d. indicazione delle copie di sicurezza;
4. mantenere e rendere accessibile un archivio dei programmi in gestione nelle eventuali diverse versioni;
5. verificare la corretta funzionalità del sistema e dei programmi in gestione;
6. adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
7. richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
8. definire e documentare le procedure da rispettare per l'apposizione del riferimento temporale;
9. verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

   Il responsabile della conservazione si vede attribuiti compiti cruciali in ragione del controllo e della supervisione che attua sull'intero procedimento di conservazione sostitutiva.

La deliberazione CNIPA 11/2004 ai commi 2 e 3 dell'art. 5 consente di delegare in tutto o in parte le attività previste ad altri soggetti interni alla struttura e/o di affidarle a soggetti terzi (pubblici o privati) i quali sono tenuti ad osservare le disposizioni contenute nella deliberazione stessa.

4.2.3.La conservazione sostitutiva dei documenti rilevanti ai fini tributari

Il decreto del Ministro dell'Economia e delle Finanze 23 gennaio 2004 dispone le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto - e riprende le disposizioni in materia di documento informatico e firma elettronica di cui al DPR. 445 del 28 dicembre 2000 (modificato dal d. Lgs 10/2002 e dal DPR 137/2003), del DPCM 8 febbraio 1999 (ora sostituito dal DPCM 13 gennaio 2004), della deliberazione

AIPA n. 42 del 13 dicembre 2001 (ora sostituita dalla deliberazione CNIPA n. 11 del 19 febbraio 2004).

Il decreto si applica, ai fini tributari (art. 2), in relazione:

1. all'emissione, conservazione ed esibizione di documenti informatici
2. alla conservazione digitale di documenti analogici

   con esclusione delle scritture e dei documenti rilevanti ai fini delle disposizioni tributarie di competenza dell'Agenzia delle Dogane.

E' stabilito che i documenti informatici rilevanti ai fini tributari devono essere (art. 3):

1. statici non modificabili, cioè non devono contenere macroistruzioni o codici eseguibili, poiché il documento dovrà essere privo di elementi che ne possano modificare la rappresentazione dopo la generazione della firma.
2. emessi con apposizione del riferimento temporale e della sottoscrizione elettronica *(ai sensi art. 1 c. 2 lett. b): sottoscrizione elettronica* intesa come *firma elettronica qualificata* ovvero *firma digitale)* essere memorizzati su un qualsiasi supporto che ne garantisca la leggibilità nel tempo purché sia assicurato l'ordine cronologico e non vi sia soluzione di continuità per ciascun periodo d'imposta: con questo si è trasposto nella norma la previsione di una tenuta delle scritture cartacee secondo le regole "dell'ordinata contabilità"
3. conservati secondo quando stabilisce la deliberazione AIPA 42/2001, che successivamente all'uscita del decreto è stata interamente sostituita con la deliberazione CNIPA 11/2004, e a cui, quindi, si deve fa- re riferimento.
4. esibiti (art. 6) presso il luogo di conservazione o per via telematica.

Per gli obbligatori che consentano funzioni di ricerca e di estrazione delle informazioni: queste chiavi di ricerca, nome, cognome, denominazione codice fiscale, partita I.V.A., data e relative associazioni logiche sono elencate nell'art. 3 comma 1 lett. d, e nulla impedisce, dopo aver rispettato questo nucleo minimo, di prevederne di ulteriori e diverse.

Per soddisfare le condizioni citate, ad esempio, nel caso di documenti in formato digitale, si deve trasformare il documento iniziale in uno statico, ovvero non con- tenente macroistruzioni o altro codice eseguibile, adottando il formato più adeguato, ad esempio un .pdf già largamente utilizzato dalle imprese.

Si procede, poi, alla memorizzazione del documento su un idoneo supporto e si attua la procedura per la conservazione. Questa termina con l'apposizione della firma digitale del responsabile della conservazione, che attesta la correttezza del processo, e della marca temporale (in luogo del riferimento temporale) che dà certezza al momento temporale, sull'insieme dei documenti ovvero su

un'evidenza informatica contenente l'impronta o le impronte dei documenti o di insiemi di essi.

La procedura, nel caso di documenti analogici acquisiti dal sistema informatico, tranne l'iniziale trasformazione del documento per il passaggio da un tipo di sup- porto ad un altro mediante uno scanner, è analoga. Nel caso in cui il documento analogico fosse in origine un documento originale unico, ovvero un documento di cui non sia possibile risalire al contenuto neanche attraverso altre scritture o do- cumenti di cui sia obbligatoria la conservazione anche presso terzi, è richiesto l'ulteriore intervento da parte di un pubblico ufficiale.

La cadenza per la conservazione sostitutiva dei documenti rilevanti ai fini tributari prevede una periodicità almeno quindicinale per le fatture e almeno annuale per i restanti documenti.

4.2.4.La fatturazione elettronica

Per la particolare tipologia di documento in oggetto a partire dall'anno 2004 è possibile usufruire dell'opportunità prevista dalla legge che permette di rendere automatico tutto il flusso di questo documento.

Il decreto Lgs. 52 del 20 febbraio 2004 consente alle aziende ed alle pubbliche amministrazioni di predisporre un innovativo sistema di fatturazione elettronica.

Con il decreto Lgs. 52/2004, emanato in attuazione della direttiva europea 2001/115/CE e sulla base della legge delega n. 14 del 3/02/2003 (legge comuni- taria 2002), oltre alla modifica integrale dell'art. 21 del DPR. n. 633/1972, disciplinante l'obbligo di fatturazione delle operazioni, si è intervenuto sugli artt. 39 e 52 dello stesso DPR, rispettivamente riguardanti la tenuta e conservazione dei regi- stri e dei documenti e l'esecuzione di accessi, ispezioni, verifiche.

Il decreto Lgs 52/2004 consente una emissione totalmente informatica della fattu- ra; l'emissione è consentita in via cartacea (modalità tradizionale) o elettronica.

La fattura elettronica, documento informatico, necessita che vi sia garanzia della provenienza del documento da parte di chi l'ha emessa. Oltre a questo, deve es- sere garantita la non alterazione del contenuto e l'attestazione della data.

Infatti, secondo quanto riportato nel decreto Lgs. 52/2004 e nella relativa circ. 45/E del 19 ottobre 2005, l'emittente deve assicurare:

1. l'attestazione della data
2. l'autenticità dell'origine
3. l'integrità del contenuto.

Per questi motivi vengono apposte sulle singole fatture il riferimento temporale e la firma digitale dell'emittente; nel caso particolare di un insieme di fatture inviate per via elettronica ad uno stesso destinatario l'apposizione della firma digitale e del riferimento digitale è consentita sull'insieme dei documenti.

Le fatture elettroniche trasmesse o ricevute in forma elettronica vanno archiviate nella stessa forma; le fatture elettroniche consegnate o spedite in via cartacea possono essere archiviate in forma elettronica. La terminologia che la norma usa, archiviazione, in questo frangente, è imprecisa poiché a seguito della trasmissio- ne della fattura elettronica e della sua eventuale archiviazione si dovrà procedere alla sua conservazione (D. Lgs. 52/2004 art. 2 comma 1), come chiarito nella cir- colare 45/E del 19 ottobre 2005 (par. 3.1.1.).

La trasmissione elettronica della fattura non contenente macroistruzioni né codi- ce eseguibile è consentita previo accordo con il destinatario.

In assenza del predetto accordo non si attua tra mittente e destinatario una fattu- razione elettronica in senso stretto, senza che questo infici la possibilità dell'uno o dell'altro soggetto di gestire informaticamente i propri documenti di fatturazione.

La cadenza per la sua conservazione, secondo quanto stabilisce il decreto del Ministero dell'Economia e delle Finanze 23 gennaio 2004, sarà quindicinale. Ai sensi dell'art. 3 DMEF 23 gennaio 2004, devono essere assicurate per i do- cumenti informatici rilevanti ai fini delle disposizioni tributarie, e, quindi, anche per le fatture, le funzioni di ricerca e di estrazione delle informazioni dagli archivi in- formatici in relazione al cognome, al nome, alla denominazione, al codice fiscale, alla partita IVA, alla data o associazioni logiche di questi ultimi.

È importante sottolineare che la fatturazione elettronica, intesa in senso stretto, non è da confondersi con la trasmissione elettronica della fattura, modalità già in passato ammessa dagli Enti competenti.

In questo caso si procede alla preparazione della fattura in formato elettronico (p.e. il già citato formato PDF) e si effettua l'invio tramite sistemi elettronici come la e-mail.

Il destinatario dovrà stampare il documento e conservarlo come se lo avesse ricevuto tramite la posta ordinaria.

4.2.5. Individuazione del luogo di conservazione

L'amministrazione, come previsto dalla normativa, potrà Conservare presso la propria sede o Affidare in Outsourcing ad altro Conservatore.

Fate le dovute considerazione l'Amministrazione effettua la Conservazione Sostitutiva presso la propria struttura informatica.

4.2.6. Il processo di conservazione: nominativi dei soggetti coinvolti

L'Amministrazione nomina il Responsabile della Conservazione interno che si occuperà delle fasi di Conservazione come previsto dalla normativa vigente. Vedi ".Documento di Nomina-"

Il responsabile della conservazione definisce le caratteristiche e i requisiti del sistema di conservazione e ne tiene evidenza in funzione della tipologia dei documenti da conservare (analogici o informatici)

Ai sensi di legge, il responsabile della conservazione appone sui lotti di archiviazione la propria firma digitale e il riferimento/marca temporale che attesta il corretto svolgimento del processo di conservazione.

Il responsabile della conservazione assicura il controllo dell'effettiva leggibilità dei documenti conservati, effettuando verifiche a cadenza periodica, comunque non superiore a cinque anni.

Il PdP supporta il responsabile della conservazione nell'archiviazione delle informazioni relative ad ogni supporto di memorizzazione utilizzato attraverso specifiche funzionalità, sulle quali egli esercita l'attività di controllo e di supervisione.

4.2.7. Responsabile della conservazione - Affidamento interno

Affidato internamente come riportato nel relativo decredto di nomina.

4.2.8. Processo di Archiviazione

Un sistema di conservazione sostitutiva richiede l'attuazione di un processo che prevede l'utilizzo di diversi strumenti e l'intervento di soggetti che concorrono a rendere l'erogazione del servizio affidabile e rispondente ai requisiti richiesti dalla legge.

Nei paragrafi che seguono sono descritte le varie fasi del processo di Archiviazione evidenziando input, output e responsabili di ogni fase. Daremo infine indicazioni sul successivo processo di Conservazione.

4.2.9. Popolamento della Base Dati

Il PdP può Archiviabile e quindi può essere Conservato un Documento che in fase di registrazione abbia un "Allegato" o un "Testo" prodotto e che sia reso immodificabile tramite applicazione dell'impronta (o HASH)

4.2.10. Applicazione dell'Impronta (o HASH)

L'Applicazione dell'impronta può avvenire durante la registrazione del documento oppure utilizzando la procedura "apponi HASH multipli" del PdP.

4.2.11. Creazione del Pacchetto di versamento

Applicata l'Impronta tramite il PdP sarà possibile generare il Pacchetto di Versamento composto da:

a) Archivio ***nomedelfile*.zip** contenente i file da archiviare e l'indice xml;
b) File di controllo del lotto ***nomedelfile*_chk.xml**
c) File di chiusura originale in chiaro ***nomedelfile*.txt**
d) File di chiusura del lotto firmato digitalmente ***nomedelfile*.txt.p7m**
e) La marca temporale associata al file di chiusura ***nomedelfile*.tsr**

4.2.12. Fasi del processo di conservazione: dettaglio

Acquisizione dei documenti da conservare

INPUT	*Documento da acquisire*	
AOO	1.1	L'UOP/UU opera sui documenti secondo le procedure previste dal PdP. Nel caso si tratti di documenti analogici cartacei procede, utilizzando uno scanner, all'acquisizione degli stessi.
OUTPUT	*Documento acquisito*	

INPUT	*Documenti da archiviare*	
AOO	2.1	I documenti vengono indicizzati e raggruppati in un unico file .zip (lotto di archiviazione) contenente anche il file indice in formato XML utilizzando le procedure previste dal PdP
OUTPUT	*Lotto di Archiviazione*	

Creazione del file di controllo e dell'impronta del documento

INPUT	*Lotto di Archiviazione*	
AOO	3.1	Del lotto di archiviazione viene generato un file di controllo in formato XML dalle procedure previste dal PdP
AOO	3.2	Del lotto di archiviazione viene generato un file di chiusura in formato TXT dalle procedure previste dal PdP
OUTPUT	*File Controllo e File di chiusura*	

Preparazione dei files da inviare alla conservazione.

INPUT	*file di chiusura .txt*	
AOO	4.1	Firmare digitalmente il file di chiusura con la vostra applicazione di firma digitale
OUTPUT	*File di chiusura firmato "**nomedelfile.txt.p7m**"*	

INPUT	*file di chiusura firmato .txt.p7m*	
AOO	5.1	Applicare la marca temporale al file di chiusura firmato come al punto 4.1 con la vostra applicazione di firma digitale
OUTPUT	*File di chiusura marcato temporalmente "**nomedelfile.tsr**"*	

INPUT	*Tutti i 5 file (come da punti 2.1, 3.1, 3.2, 4.1, 5.1)*	
Cliente	5.1	Generare un file .zip con la vostra applicazione per la compressione dei file
OUTPUT	*File da archiviare "**nomedelfile.zip**"*	

4.2.13. Invio al sistema di conservazione

Inviare l'archivio così creato al sistema di conservazione interno.

4.2.14. Responsabilità

Nel processo di conservazione sostitutiva intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Attività Responsabilità	UU/Operatore	Responsabile Conservazione
1. Acquisizione del documento da conservare	E-V	
2. Creazione della prima versione del pacchetto di archiviazione	E-V	
3. Creazione del file di controllo e dell'impronta del documento	E-V	
4. firma e marcatura temporale dei file		E - V
5. Creazione del pacchetto di archiviazione definitivo		E - V
7. invio al sistema di conservazione interno		E - V

8. invio al sistema di conservazione esterno		E - V
10. Memorizzazione, creazione "copia di sicurezza" e chiusura del processo		E - V

[**E**-esegue; **V**- verifica]

4.2.15. Identificazione nel PdP

Il responsabile della conservazione viene identificato nel sistema PdP grazie alla definizione di un particolare utente "responsabile del procedimento di conservazione", riconosciuto tramite autenticazione. Gli estremi identificativi di questo particolare utente (organizzazione di appartenenza, cognome, nome e codice fiscale) sono, inoltre, riportati anche nelle informazioni associate ai documenti conservati (nelle informazioni relative ad ogni documento e nel file di chiusura del lotto).

4.2.16. Archivi – PdP

La definizione del sistema di archiviazione e conseguente Conservazione Sostitutiva offre l'opportunità di poter avere a disposizione e utilizzare due diverse fonti (archivi) da cui poter ricavare le informazioni e/o i documenti di interesse.

Tipo archivio	
	Descrizione
Archivio di "lavoro"	Permette un agevole recupero dei documenti necessari per una consultazione legata a mere necessità operative e/o di verifica interne utilizzando le procedure Documentali PdP
Archivio a norma	Permette il recupero e l'esibizione dei documenti già sottoposti al processo di conservazione, garantendo la possibilità di ottenere il documento corredato di tutte le informazioni da opporre in caso di verifica da parte degli Enti competenti.

4.2.17. Dati relativi ai formati dei file accettati per la conservazione

Formato	Non firmato	Firmato	Firmato e marcato	descrizione	Nome del file e visualizzatore corrispondente
PDF	Si	Si	Si	Adobe PDF	Adobe Acrobat Reader (tutti i sistemi operativi)
TIF	Si	Si	Si	Tag Image	Visualizzatore di immagini standard (tutti i sistemi operativi)
TXT	Si	Si	Si	Text Plan	Visualizzatore di testo standard (tutti i sistemi operativi)
XML	Si	Si	Si	XML	Visualizzatore XML standard (tutti i sistemi operativi)
ODS ODT ODP	Si	Si	Si	Open Office - cifrato	Open Office (tutti i sistemi operativi)
DOC PPT XLS	Si	Si	Si	Microsot Office - cifrato	Visualizzatori di Microsot Office (tutti i sistemi operativi)
JPG GIF RTF		Si	Si	Tag Image	Visualittore di immagini standard (tutti i sistemi operativi)

4.2.18. Ricerca

La ricerca dei documenti è riservata al personale che dispone delle apposite autorizzazioni e che, in base all'attribuzione dei compiti d'ufficio, deve poter prende- re visione dei dati conservati.

4.2.19. Esibizione

Una volta individuato il documento richiesto, il soggetto interessato o un suo delegato, provvede a renderlo leggibile in qualunque momento e disponibile, a richiesta, su supporto cartaceo.

4.2.20. Misure per la sicurezza fisica e logica

Per la descrizione delle infrastrutture che il PdP utilizza si rimanda al Capitolo 3.

4.2.21. Note conclusive

Indichiamo come **Luogo di Archiviazione** il luogo di archiviazione dei documenti relativi all'archivio di lavoro che è ubicato presso l'infrastruttura sopra indicata.

Indichiamo come **Luogo di conservazione** il luogo di conservazione dei documenti relativi all'archivio a norma. Il "luogo di conservazione" resta quindi nei locali del cliente.

4.3. CONSERVAZIONE DELLE REGISTRAZIONI DI SICUREZZA

Un operatore addetto alla sicurezza dell'amministrazione/AOO, con periodicità settimanale, provvede a alla memorizzazione su supporto non riscrivibile dei seguenti file di sicurezza creati e poi scaricati dal PdP.

I supporti così realizzati sono conservati in cassaforte con caratteristiche ignifughe per un periodo minimo di dieci anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

5. MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI.

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.

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

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

- ricevuto;
- inviato;
- interno formale;
- interno informale.

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

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e che "2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità".

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

5.1. DOCUMENTO RICEVUTO

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

Un documento informatico può essere recapitato:

1. a mezzo posta elettronica convenzionale o certificata;
2. su supporto rimovibile quale, ad esempio, CD ROM, DVD, pen drive, etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telefax o telegramma;
4. con consegna diretta da parte dell'interessato o consegnato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico

5.2.DOCUMENTO INVIATO

I documenti informatici, compresi di eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.

In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

5.3.DOCUMENTO INTERNO FORMALE

I documenti interni sono formati con tecnologie informatiche.

Lo scambio tra UOR/UU di documenti informatici di rilevanza amministrativa giuridico probatoria, avviene principalmente al mezzo del WorkFlow documentale del PdP o, se necessario, per mezzo della posta elettronica convenzionale, o, se disponibile, di quella certificata.

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

Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato.

5.4.DOCUMENTO INTERNO INFORMALE

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

5.5.IL DOCUMENTO INFORMATICO

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; l'art. 20 del decreto legislativo del 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" prevede che:

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente codice ed alle regole tecniche di cui all'articolo 71.
2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto

delle regole tecniche stabilite ai sensi dell'articolo 71 che garantiscano l'identificabilità dell'autore e l'integrità del documento.

3. Le regole tecniche per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico".

5.6. IL DOCUMENTO ANALOGICO - CARTACEO

Per documento analogico s'intende un documento amministrativo "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale". Di seguito faremo riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampata.

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

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel paragrafo 4.2.

5.7. FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI

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

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

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

Le firme (e le sigle se si tratta di documento analogico) necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabili dei singoli UOR.

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

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

Il documento deve inoltre recare almeno le seguenti informazioni:

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

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

5.8. SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI

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

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

I documenti informatici prodotti dall'amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma

digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

5.8.1. DOCUMENTI DA SOTTOSCRIVERE CON FIRMA DIGITALE

Tutti i documenti prodotti che necessitano di firma da parte dei possessori di firma digitale.

5.8.2. DOCUMENTI DA SOTTOSCRIVERE CON FIRMA QUALIFICATA

Tutti i documenti prodotti che necessitano di firma da parte di chi non è in possesso di firma digitale.

5.8.3. DOCUMENTI CHE NON NECESSITANO DI ALCUNA FIRMA ELETTRONICA

Qualsiasi documento diverso da quelli indicati nei due precedenti paragrafi.

5.9. REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO

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

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno dellA AOO;
- l'interconnessione tra le UOP/UOR e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

5.10. FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 5.9 è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per

sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità.

Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito www.cnipa.gov.it).

5.11. VERIFICA DELLE FIRME CON IL PDP

Nel PdP non prevede funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare ma richiede l'utilizzo di software stand-alone fornito dalle società di certificazione. L'amministrazione si avvale del software **ArubaSign.**

La sequenza delle operazioni previste è la seguente:

- apertura della busta "virtuale" contenente il documento firmato[2];
- verifica della validità del certificato. Questa attività è realizzata con **ArubaSign**;
- verifica della firma (o delle firme multiple) con **ArubaSign**;
- verifica dell'utilizzo nella apposizione della firma di un certificato utente emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati, e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate al CNIPA con la periodicità richiesta dal software **ArubaSign**;
- Se necessario, trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF o XML o TIFF) e attribuzione della segnatura di protocollo;
- inserimento, nel sistema documentale del PdP o dell'AOO, sia del documento originale firmato, sia del documento in chiaro qualora fosse necessario;

5.12. USO DELLA POSTA ELETTRONICA CERTIFICATA

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

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

---

[2] La busta "virtuale" è costruita secondo la standard PKCS#7 e contiene il documento, la firma digitale ed il certificato rilasciato dalla autorità di certificazione unitamente alla chiave pubblica del sottoscrittore del documento.

Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura o con gli strumenti di editing previsti dal PdP;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno, che sono classificati in:

- conferma di ricezione;
- notifica di eccezione;
- aggiornamento di conferma;
- annullamento di protocollazione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Il servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via

telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

6. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

6.1. GENERALITÀ

I flussi di lavorazione dei documenti all'interno della AOO si riferiscono ai documenti:

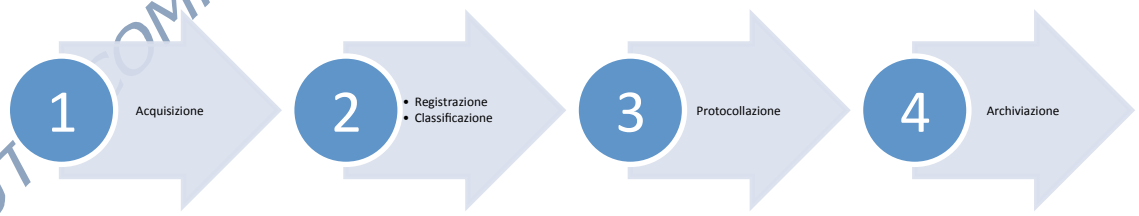
- ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;
- inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

Come previsto dalla normativa vigente i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.

I flussi relativi alla gestione dei documenti all'interno dell'AOO sono descritti graficamente nel paragrafo seguente prendendo in esame quelli che possono avere rilevanza giuridico-probatoria.

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.

6.2. FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO



1. L'acquisizione del documento avviene attraverso il sistema PdP. In caso di documento Analogico questo viene precedentemente digitalizzato in formato PDF. In caso di messaggio di Posta Elettronica Ordinaria o Certificata questa viene automaticamente immessa nel PdP nel formato aperto .eml inglobando tutte le caratteristiche fisiche e logiche della stessa inclusi gli allegati;
2. La registrazione e la classificazione secondo i contenuti minimi previsti dalle regole di protocollo avvengo attraverso il PdP;

3. Il PdP assegna numero di protocollo e genera la segnatura di protocollo assegnando un codice Hash (contenente l'impronta digitale della registrazione e del documento informatico) che rende immodificabile tutta la registrazione;
4. La conferma di registrazione inserisce nell'archivio corrente.

6.2.1. REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

La protocollazione e la segnatura della corrispondenza in arrivo, sia essa in formato digitale che in formato analogico, è effettuata direttamente dal UOP.

Vengono effettuate le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura.

Il documento registrato presso il protocollo riservato è individuato dall'appartenenza al Gruppo Utente "196" e non ne viene data nessuna evidenza.

6.2.2. PROVENIENZA ESTERNA DEI DOCUMENTI

I documenti che sono trasmessi da soggetti esterni all'amministrazione sono, oltre quelli richiamati nel capitolo precedente, i telefax, i telegrammi e i supporti digitali rimovibili. Questi documenti sono recapitati alla/e UOP designata/e.

I documenti che transitano attraverso il servizio postale sono ritirati quotidianamente secondo le seguenti regole:

1. *La corrispondenza viene quotidianamente raccolta dal servizio postale pubblico da un collaboratore scolastico alle ore 11.00 di ogni giorno;*

6.2.3. PROVENIENZA DI DOCUMENTI INTERNI FORMALI

Per sorgente interna dei documenti si intende qualunque RPA che invia formalmente la propria corrispondenza alla UOP della AOO per essere a sua volta nuovamente trasmessa, nelle forme opportune, ad altro UOR o UU della stessa AOO.

Il documento è di tipo informatico secondo i formati standard illustrati nel precedente capitolo.

Il mezzo di recapito è il WorkFlow documentale del PdP.

Nella fase transitoria verso la diffusione della digitalizzazione dell'amministrazione, i documenti interni possono essere anche di tipo analogico.

In questo caso il mezzo di recapito del documento può essere il servizio di posta interna.

6.2.4.RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ISTITUZIONALE

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo al UOP in cui si è organizzata l'AOO.

Quando i documenti informatici pervengono alle UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento procede alla registrazione di protocollo per come indicato nel paragrafo 6.2.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente ovvero non siano dotati di firma elettronica e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio è inserito nel sistema di gestione documentale con il formato di origine apponendo nel campo di classificazione del PdP aggiuntiva "connettore posta" e successivamente protocollato, smistato, assegnato e gestito. 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 amministrativo (RPA);

L'addetto protocollatore controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e verifica se sono da protocollare.

6.2.5.RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ELETTRONICA NON ISTITUZIONALE

Nel caso in cui il messaggio viene ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio viene inoltrato alla casella di posta istituzionale e inviando un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta. I controlli effettuati sul messaggio sono quelli sopra richiamati.

6.2.6.RICEZIONE DI DOCUMENTI INFORMATICI SU SUPPORTI RIMOVIBILI

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.

Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti

informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

6.2.7. RICEZIONE DI DOCUMENTI CARTACEI A MEZZO POSTA CONVENZIONALE

I documenti pervenuti a mezzo posta o ritirati dal personale della UOP dagli uffici postali sono consegnati alla UOP.

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

La corrispondenza relativa a bandi di gara è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.

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

La corrispondenza ricevuta via telegramma o via telefax o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo.

Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

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

6.2.8. DOCUMENTI CARTACEI RICEVUTI A MEZZO POSTA CONVENZIONALE E TUTELA DEI DATI PERSONALI

L' UOR sono aperte pubblico secondo gli orari di uffici indicati. Se per errore la corrispondenza viene recapitata ad un UOR quest'ultimo, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente nelle forme stabilite dal RSP, e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UOP abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.

Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.

6.2.9.ERRATA RICEZIONE DI DOCUMENTI DIGITALI

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

6.2.10. ERRATA RICEZIONE DI DOCUMENTI CARTACEI

Nel caso in cui pervengano erroneamente alla UOP dell'amministrazione documenti indirizzati ad altri soggetti:

a) si restituisce alla posta;
b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto e nel campo di classificazione del PdP una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

6.3.FLUSSO DEI DOCUMENTI INVIATI DALLA AOO

1. La generazione del documento avvine con gli strumenti di Office Automation in uso all'Amministrazione, o con le funzioni di PrintMerge ed editing forniti dal PdP;
2. La registrazione e la classificazione secondo i contenuti minimi previsti dalle regole di protocollo avvengo attraverso il PdP;
3. Il documento prodotto viene indirizzato attraverso il Sistema di Work Flow Documentale del PpP per la revisione e/o apposizione delle firme digitali o qualificata;
4. Formato il Documento in partenza il PdP assegna numero di protocollo e genera la segnatura di protocollo e la il codice Hash contenente l'impronta digitale della registrazione e del documento informatico rendendo immodificabile la registrazione;
5. La conferma di registrazione inserisce nell'archivio corrente

6. Spedizione

6.3.1.DOCUMENTI IN PARTENZA

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione o altra AOO della stessa amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti capitoli.

I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.

Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo caso sono il servizio postale, nelle sue diverse forme, ed il servizio telefax.

6.3.2. VERIFICA FORMALE DEI DOCUMENTI

Ogni UOR è autorizzata dall'AOO per il tramite del RSP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita.

Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR.

Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

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

6.3.3. REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UU/UOR abilitati in quanto collegati al PdP della AOO.

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

Il documento registrato presso il protocollo riservato è individuato dall'appartenenza al Gruppo Utente "196" e non ne viene data nessuna evidenza.

6.3.4. TRASMISSIONE DI DOCUMENTI INFORMATICI

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AIPA 7 maggio 2001, n. 28.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dal CNIPA.

Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

6.3.5. TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO POSTA

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici

Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP secondo le seguenti regole:

1. *Gli Uffici Utente devono far pervenire la posta in partenza all'Ufficio Posta della UOP generale che esegue la spedizione, entro e non oltre le ore 11:00 di ogni giorno lavorativo.*
2. *La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, o… viene consegnata in busta chiusa al servizio postale pubblico alle ore 11.00. (o in alternativa, in occasione della raccolta della corrispondenza) di ogni giorno;*

6.3.6. TRASMISSIONE DI DOCUMENTI CARTACEI A MEZZO TELEFAX

Sul documento trasmesso via fax può essere apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale".
Solo su richiesta del destinatario verrà trasmesso anche l'originale.
Le ricevute della avvenuta trasmissione sono trattenute, temporaneamente, dalla UOP che ha effettuato la trasmissione.

6.3.7. CIRCOLARI E DISPOSIZIONI GENERALI

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.
I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

6.3.8. DOCUMENTI CARTACEI IN PARTENZA CON PIÙ DESTINATARI

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale con la dicitura "Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari - Vedi elenco allegato alla minuta/copia presso l'UOR/UU/RPA".
Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

6.3.9. INSERIMENTO DELLE RICEVUTE DI TRASMISSIONE

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno Sistema Documentale con una registrazione a cura del PdP e collegamento informatico al documento che le ha generate.
Gli UOR che effettuano la spedizione di documenti informatici o cartacei direttamente curano anche l'archiviazione delle ricevute di ritorno.

7. ATTIVITÀ DI PROTOCOLLAZIONE DEI DOCUMENTI

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

7.1. REGISTRO GIORNALIERO DI PROTOCOLLO

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato entro le ore 24 del giorno successivo alla Conservazione Sostitutiva

È a carico del Responsabile della Conservazione Sostitutiva conservare in modalità sicura la copia del registro giornaliero di protocollo.

7.2. REGISTRAZIONE DI PROTOCOLLO

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

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento, registrato in forma non modificabile;
- il destinatario del documento, registrato in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la classificazione.

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

Tali dati facoltativi sono descritti nei paragrafi seguenti.

7.2.1. DOCUMENTI INFORMATICI

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

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

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

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

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

Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

7.2.2. DOCUMENTI ANALOGICI (CARTACEI E SUPPORTI RIMOVIBILI)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP).

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

Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

7.2.3. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI

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

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo inequivocabile.

a) DOCUMENTI INFORMATICI

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche
dell'Extensible Markup Language (XML).
Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del documento.

È facoltativo riportare anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo.

Per i documenti informatici in partenza, possono essere specificate, in via facoltativa, anche le seguenti informazioni:

- persona o ufficio destinatario;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.
Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.
L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.
Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal CNIPA, includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

b) DOCUMENTI CARTACEI

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

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

Facoltativamente possono essere riportate anche le seguenti informazioni:

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

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

L'AOO ha optato per il "segno" riportato nell'allegato 16.22.

L'operazione di segnatura dei documenti in partenza viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dalla UOP.

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

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

7.3. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

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

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

Solo il RSP è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RSP.

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

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

7.4. LIVELLO DI RISERVATEZZA

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.

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

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

7.5. REGISTRAZIONI DI PROTOCOLLO PARTICOLARI (RISERVATE)

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

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;

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

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

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

7.6. DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEGRAMMA

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

7.7. DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.

Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.

L'accertamento della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.

Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RPA provvede ad acquisire l'originale.

Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "Già pervenuto via fax il giorno……".

Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso.

Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione.

Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax".

Il documento in partenza reca una delle seguenti diciture:

- "Anticipato via telefax" se il documento originale viene successivamente inviato al destinatario;
- "La trasmissione via fax del presente documento non prevede l'invio del documento originale » nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta;

La segnatura viene apposta sul documento e non sulla copertina di trasmissione.
La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.
Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche.
In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura secondo gli standard XML vigenti e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

7.8. DOMANDE DI PARTECIPAZIONE A CONCORSI, AVVISI, SELEZIONI, CORSI E BORSE DI STUDIO

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.
Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.
Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

7.9. PROTOCOLLAZIONE DI DOCUMENTI INERENTI A GARE DI APPALTO CONFEZIONATI SU SUPPORTI CARTACEI

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

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

Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

7.10. DOCUMENTI NON FIRMATI

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

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

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

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

7.11. PROTOCOLLAZIONE DEI MESSAGGI DI POSTA ELETTRONICA CONVENZIONALE

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

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;
- in caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale, il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

7.12. PROTOCOLLO DI DOCUMENTI DIGITALI PERVENUTI ERRONEAMENTE

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'amministrazione non competente, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

7.13. RICEZIONE DI DOCUMENTI CARTACEI PERVENUTI ERRONEAMENTE

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'amministrazione, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

7.14. COPIE PER CONOSCENZA

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nella precedente lettera "l". In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza.
Tale informazione è riportata anche sulla segnatura di protocollo.

7.15. DIFFERIMENTO DELLE REGISTRAZIONI

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre il giorno lavorativo successivo dal ricevimento di detti documenti.
Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

7.16. REGISTRAZIONI DI DOCUMENTI TEMPORANEAMENTE RISERVATI

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

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

7.17. CORRISPONDENZA PERSONALE O RISERVATA

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

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

7.18. INTEGRAZIONI DOCUMENTARIE

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

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

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

7.19. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL PDP

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

Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

7.19.1. ATTRIBUZIONE DEL PROTOCOLLO

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il servizio di protocollo è realizzato dall'applicativo PdP attraverso l'apposizione di un riferimento temporale come previsto dalla normativa vigente.

Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.

Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili. E giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

7.19.2. REGISTRO INFORMATICO DI PROTOCOLLO

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO si provvede, in fase di chiusura dell'attività di protocollo, ad effettuare le seguenti operazioni:

- estrazione delle registrazioni del giorno precedente dal file del registro generale di protocollo;
- applicazione della firma digitale e di un riferimento temporale al file così realizzato;
- copia del file estratto, del file di firma e del riferimento temporale su supporto rimovibile non riscrivibile;
- salvataggio del file di firma e del riferimento temporale sul sistema di esercizio del PdP.

Riversamento nel sistema di Conservazione Sostitutiva.

7.19.3. RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI INFORMATICI

La ricezione di documenti comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica.

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

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

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

7.19.4. RILASCIO DI RICEVUTE ATTESTANTI LA RICEZIONE DI DOCUMENTI CARTACEI

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

La semplice apposizione del timbro datario dell'UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell'UOP in merito alla ricezione ed all'assegnazione del documento.

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata ad una UOP di protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a:

- Inviare alla posta elettronica la ricevuta di protocollo a seguito di archiviazione.
- apporre sul modulo specifico di ricevuta realizzato dal PdP Il numero di protocollo, la data e l'ora d'arrivo, il nome dell'operatore incaricato.

7.20. CONSERVAZIONE DEI DOCUMENTI INFORMATICI

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo. I documenti ricevuti per via telematica sono resi disponibili agli UU attraverso l'uso del Work Flow Documentale del PdP subito dopo l'operazione di smistamento e di assegnazione.

7.21. CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.

Il processo di scansione avviene in diverse fasi:

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

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

I documenti cartacei dopo l'operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della delibera CNIPA 19 febbraio 2004 n.11 vengono inviati agli UOR/UU/RPA destinatari per le operazioni di fascicolazione e conservazione.

- In ogni caso non vengono riprodotti in formato immagine i seguenti documenti:
  - i certificati medici contenenti la diagnosi,

Le UOP/UU abilitate all'operazione di scansione dei documenti sono riportate nell'allegato 2 "-AOO-"

7.22. CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO DEI DOCUMENTI

Gli addetti alla UOP provvedono ad inviare il documento al Dirigente Scolastico che identifica l'UOR di destinazione. Quest'ultimo:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore rinvia il documento all'ufficio smistamento di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione in essere presso l'amministrazione.

7.23. CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

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

8. REGOLE DI SMISTAMENTO E D ASSEGNAZIONE D E I DOCUMENTI RICEVUTI

Il presente capitolo riporta le regole di smistamento ed assegnazione dei documenti ricevuti.

8.1. REGOLE DISPONIBILI CON IL PDP

L'attività di smistamento consiste nell'operazione di inviare, tramite WorkFlow Documentale, un documento protocollato e segnato all'UOR competente in base alla classificazione di primo livello del titolario, documento.

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

Effettuato lo smistamento e l'assegnazione, il RPA provvede alla presa in carico del documento allo stesso assegnato.

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

L'UOR competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.

I documenti che sono immediatamente riconducibili ad una specifica UOR e/o materia, vengono inoltrati direttamente dalla UOP.

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

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

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

Nell'allegato 2 "-AOO-" sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.

Nello stesso allegato, per ciascuna delle strutture in elenco, sono indicati:

- l'indirizzo elettronico;
- le principali tipologie di documenti trattati che determinano i criteri di assegnazione della corrispondenza.

Tutta la corrispondenza protocollata nell'arco della giornata viene inviata in visione al Preside affinché possa valutarla apportando eventuali modifiche o correzioni.

La corrispondenza ritorna alla/e UOP mittente/i per le eventuali correzioni e/o integrazioni e per l'assegnazione del documento precedentemente protocollato e segnato.

8.2. CORRISPONDENZA DI PARTICOLARE RILEVANZA

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione a DSGA e al DS che provvede ad individuare l'UOR competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

8.3. ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO ELETTRONICO

I documenti ricevuti dall'AOO sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile.

L'UOR competente ha notizia dell'arrivo della posta ad esso indirizzata tramite una assegnazione di WorkFlow dal PdP.

Il responsabile dell'UOR può visualizzare i documenti, attraverso l'utilizzo del PdP e in base alle abilitazioni previste potrà:

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

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

I destinatari del documento per "competenza" lo ricevono esclusivamente in formato digitale.

8.4. ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO

I documenti ricevuti dall'amministrazione in formato cartaceo, se successivamente acquisiti in formato immagine con l'ausilio di scanner, una volta concluse le operazioni di registrazione, di segnatura e di assegnazione, sono fatti pervenire al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione/AOO. L'originale cartaceo può essere successivamente trasmesso al RPA oppure essere conservato dalla UOP.

La procedurà è la stessa adottata per i Documenti Digitali.

8.5. MODIFICA DELLE ASSEGNAZIONI

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento, se è abilitato all'operazione di smistamento, provvede a trasmettere l'atto all'UOR competente, in

caso contrario comunica l'errore alla UOP che ha erroneamente assegnato il documento, che procederà ad una nuova assegnazione.

Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenza attribuite ad altro UU dello stesso UOR, l'abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UOR medesima o a persona da questi incaricata.

Il PdP tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

9. GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI – WORK-FLOW

Quanto di seguito riportato in termini di base informativa dei procedimenti amministrativi dell'amministrazione/AOO, costituisce il riferimento per qualsiasi successivo impiego delle tecnologie informatiche di gestione dei flussi documentali (work flow).

9.1. AVVIO DEI PROCEDIMENTI E GESTIONE DEGLI STATI DI AVANZAMENTO

Mediante l'assegnazione dei fascicoli agli UOR/UU di volta in volta competenti, le UOP o i RPA provvedono a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente.

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

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

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

10. ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE E DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE.

10.1. DOCUMENTI ESCLUSI

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

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)

Sono inoltre esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000, n. 445.

10.2. DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti:

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;

- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241; dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti.

11. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Il presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal PdP.

11.1. IL REGISTRO DI EMERGENZA

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

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

Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RSP annota sullo stesso il mancato uso.

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

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

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.

A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

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

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

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

11.2. MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea.

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

Per semplificare e normalizzare la procedura di apertura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) che riporta oltre all'identificazione dell'amministrazione e della AOO:

1. Causa dell'interruzione,
2. Data e ora di inizio interruzione,
3. Data e ora fine interruzione
4. Numero protocollo d'Inizio
5. Numero protocollo di fine.
6. Numero di pagina
7. Firma del responsabile

L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 2 "-AOO-".

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

11.3. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo generale.

Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico (o persona da lui delegata) provvede a tener informato il RSP sui tempi di ripristino del servizio

11.4. MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA

È compito del RSP verificare la chiusura del registro di emergenza.

È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.

Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

Per semplificare la procedura di chiusura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) analogo a quello utilizzato nella fase di apertura del registro di emergenza.

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

12.1. MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO DEL MANUALE

L'amministrazione adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico (RSP).

Il presente Manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal RSP.

12.2. REGOLAMENTI ABROGATI

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

12.3. PUBBLICITÀ DEL PRESENTE MANUALE

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1900, n. 241, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento. Inoltre copia del presente Manuale è:

- fornito a tutto il personale dell'AOO e se possibile resa disponibile mediante la rete intranet;
- inviata all'organo di revisione;
- pubblicata sul sito internet dell'amministrazione.

12.4. OPERATIVITÀ DEL PRESENTE MANUALE

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