

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO

INDICE

SEZIONE I: Contenuti Generali.....	3
Articolo 1: Finalità	3
Articolo 2: Ambito di applicazione	4
Articolo 3: Struttura del Manuale.....	5
Articolo 4: Infrastruttura tecnologica e applicativa.....	7
Articolo 5: Sigle e definizioni	8
Articolo 6: Modalità di comunicazione alla Comunità Amministrata	10
SEZIONE II: Contenuti Organizzativi.....	11
Articolo 7: Obiettivi di adeguamento alla normativa	11
Articolo 8: Accredimento dell'Amministrazione	11
Articolo 9: Area Organizzativa Omogenea.....	11
Articolo 10: Struttura e compiti di SPI	12
Articolo 11: Responsabile di SPI e suo vicario.....	13
Articolo 12: Struttura e compiti del SIA	13
Articolo 13: Responsabile del SIA e suo vicario.....	13
Articolo 14: Compiti del SIA particolarmente rilevanti	13
Articolo 15: Responsabile della Sicurezza dei Dati Personali e suo vicario.....	14
Articolo 16: Unità Organizzative Responsabili	14
Articolo 17: Modello organizzativo adottato nella gestione dei documenti	14
Articolo 18: Misure tecniche ed organizzative per l'eliminazione dei protocolli separati	15
SEZIONE III: Strumenti Archivistici	16
Articolo 19: Quadro di classificazione	16
Articolo 20: Trasferimento dei documenti nell'archivio di deposito.....	16
Articolo 21: Trasferimento dei documenti nell'archivio storico	16
Articolo 22: Piano di conservazione dell'archivio	16
Articolo 23: Regolamentazione dell'accesso all'archivio	17
SEZIONE IV: Organizzazione della Gestione dei Documenti.....	18
Articolo 24: Fasi rilevanti della gestione dei documenti.....	18
Articolo 25: Produzione.....	19
Articolo 26: Ricezione	20
Livelli di riservatezza	21
Procedura di "preassegnazione" per la verifica di accettabilità del documento.....	21
Procedura di rifiuto	23
Articolo 27: Protocollazione e classificazione	23
Registrazione	24
Segnatura (Timbro di protocollo).....	24
Unicità del numero di protocollo	24
Classificazione	24
Scansione Ottica	25
Documenti soggetti ad obbligo di protocollazione	25
Annullamento o modifica di una registrazione.....	26
Registro giornaliero di protocollo	27

Registro di emergenza	29
Articolo 28: Fascicolazione	30
Documenti in arrivo	31
Documenti in partenza	31
Repertorio dei fascicoli	32
Articolo 29: Spedizione	32
Articolo 30: Archiviazione e conservazione.....	32
Selezione	33
Versamento.....	33
Le serie archivistiche.....	33
L'archivio storico.....	33
SEZIONE V: Flussi di Lavorazione dei Documenti.....	34
Articolo 31: Distribuzione con assegnazione dei documenti in arrivo	34
Articolo 32: Gestione integrata dei fascicoli, dei flussi documentali e dei procedimenti amministrativi.....	35
SEZIONE VI: Accessibilità e Sicurezza dei Documenti.....	36
Articolo 33: Caratteristiche del Piano della Sicurezza dei Documenti Informatici	36
Articolo 34: Analisi dei rischi	36
Articolo 35: Accesso fisico agli uffici di SPI, SIA e delle UOR.....	37
Articolo 36: Livelli di riservatezza.....	37
Articolo 37: Profili utente e autorizzazioni d'accesso	38
Articolo 38: Password	39
Articolo 39: Clear screen e clear desk policy	40
Articolo 40: Le stampe	40
Articolo 41: Protezione da software malizioso e da intrusioni esterne	41
Articolo 42: Salvataggio dei dati correnti.....	41
Casella di Posta Elettronica Istituzionale.....	42
Archivio corrente	42
Articolo 43: Misure per la continuità del servizio	43
Misure a carico di SPI	43
Misure a carico delle UOR	43
Articolo 44: Tracciamento delle operazioni	44
Articolo 45: Produzione.....	44
Articolo 46: Ricezione	45
Articolo 47: Protocollazione e classificazione	45
Articolo 48: Fascicolazione	45
Articolo 49: Spedizione	46
Articolo 50: Archiviazione e conservazione.....	46
Articolo 51: Gestione dei flussi documentali	47
SEZIONE VII: Tempificazione dell'intervento	48
Articolo 52: Prima fase di attuazione.....	48
Articolo 53: Seconda fase di attuazione.....	48

SEZIONE I: Contenuti Generali

Articolo 1: Finalità

Il Manuale di Gestione dei Documenti, di seguito indicato più brevemente come MANUALE, descrive, ai sensi dell'art. 5 del DPCM 31 Ottobre 2000, il sistema di gestione e conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del Servizio per la tenuta del Protocollo Informatico, della Gestione dei Flussi Documentali e degli Archivi. Il Servizio, di seguito indicato con la sigla **SPI**, ha la struttura ed i compiti descritti nell'Art. 10 della Sez. II.

Riportiamo nel seguito le funzioni particolari svolte dal MANUALE indicando fra parentesi, al termine di ogni punto contrassegnato dalle lettere da a) ad o), il riferimento alle sue parti (sezioni, articoli od allegati) che le trattano in modo prevalente:

a) la definizione, su indicazione del responsabile di **SPI**, dei tempi, delle modalità e delle misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal decreto del Presidente della Repubblica n. 428/1998 (**Sezione II - Articolo 18**);

b) il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il responsabile dei Sistemi Informativi Automatizzati e con il responsabile della Sicurezza dei Dati Personali di cui alla legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, e nel rispetto delle misure minime di sicurezza previste dal regolamento di attuazione emanato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318, in attuazione dell'art. 15, comma 2, della citata legge n. 675/1996 (**Sezione VI e Allegato 6**);

c) le modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'Area Organizzativa Omogenea (**Allegato 1**);

d) la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione, tra i quali, in particolare, documenti informatici di fatto pervenuti per canali diversi da quelli previsti dall'art. 15 del DPCM 31 Ottobre 2000, nonché fax, raccomandata, assicurata (**Sezione IV**);

e) l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione e/o verso altre amministrazioni (**Sezione V**);

f) l'indicazione delle Unità Organizzative Responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'Area Organizzativa Omogenea (**Sezione II – Articolo 16 e Allegato 3**);

g) l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 4, comma 5, del decreto del Presidente della Repubblica n. 428/1998 (**Sezione IV – Articolo 27**);

h) l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento (**Sezione IV – Articolo 27**);

i) il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, anche con riferimento all'uso di supporti sostitutivi (**Sezione III e Allegato 5**);

l) le modalità di produzione e di conservazione delle registrazioni di protocollo informatico ed in particolare l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire la non modificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione di segnatura ai sensi dell'art. 6 del decreto del Presidente della Repubblica n. 428/1998, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione (**Sezione IV – Articolo 27**);

m) la descrizione funzionale ed operativa del sistema di protocollo informatico con particolare riferimento alle modalità di utilizzo (**Sezione IV**);

n) i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali (**Sezione VI – Articolo 37**);

o) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 14 del decreto del Presidente della Repubblica n. 428/1998, inclusa la funzione di recupero dei dati protocollati manualmente (**Sezione IV – Articolo 27**).

Il MANUALE costituisce lo strumento di lavoro che l'Amministrazione mette a disposizione di tutto il personale come supporto alla gestione dei documenti, degli affari e dei procedimenti amministrativi che è chiamato a trattare in tutte le sue componenti. In particolare, il MANUALE descrive le fasi operative del sistema per la gestione del protocollo informatico, dei flussi documentali e degli archivi specificando per ogni attività i rispettivi livelli di esecuzione, responsabilità e controllo.

Lo stesso MANUALE, quando è reso pubblico secondo quanto previsto dalla normativa, assume nei confronti della Comunità Amministrata la funzione di Carta dei servizi; a questo riguardo si veda anche il contenuto dell'Art. 4 della Sez. I.

Articolo 2: Ambito di applicazione

L'ambito di applicazione del MANUALE per ciò che attiene ai documenti in arrivo comprende tutti e solo i documenti soggetti a protocollazione, mentre per i documenti prodotti dall'Amministrazione, siano essi quelli interni aventi valenza giuridica o rilevanti ai fini dell'azione amministrativa che quelli prodotti ed indirizzati a destinatari esterni all'Area Organizzativa Omogenea, di seguito indicata con la sigla **AOO**, riguarda esclusivamente i documenti redatti in versione definitiva sottoscritta soggetti a protocollazione. Pertanto il MANUALE non si occupa specificamente di disciplinare le fasi preparatorie dei documenti né relativamente ai processi di produzione all'interno delle singole Unità Organizzative Responsabili, di seguito indicate con la sigla **UOR**, né relativamente agli scambi di

informazioni documentali fra diverse **UOR** effettuate al fine di produrre i documenti. Ciò nonostante, l'Amministrazione ritiene utile sottolineare che, sia il trattamento dei documenti in arrivo non soggetti a protocollazione, che i trattamenti documentali intermedi della fase di produzione realizzati nell'ambito delle **UOR**, dovranno essere comunque effettuati con modalità in accordo ai principi generali espressi dal Piano della Sicurezza dei Documenti Informatici previsto dal MANUALE.

Articolo 3: Struttura del Manuale

Il MANUALE è strutturato in due componenti distinte ed integrate: un testo e gli allegati. Il testo contiene tutte le disposizioni ed i principi di carattere generale che costituiscono un corpo tendenzialmente inalterato nel tempo pur con componenti differenziate in termini di tempificazione di operatività come indicato nella Sez. VII. Viceversa, gli allegati contengono informazioni e disposizioni di natura tecnica e operativa inerenti al contesto organizzativo e tecnologico che non pregiudicano in alcun modo i principi espressi nel testo, ma li interpretano e calano nel divenire dell'organizzazione dell'Ente. Come tali, gli allegati possono necessitare di aggiornamenti continui, specialmente nella prima fase di applicazione del MANUALE. A questo scopo l'Amministrazione si riserva di rilasciare specifiche autorizzazioni ed assegnare compiti inerenti al loro aggiornamento periodico.

Il testo del MANUALE è organizzato in sette Sezioni numerate con numeri romani. Ogni Sezione è suddivisa in Articoli numerati progressivamente all'interno della stessa Sezione. Per esclusiva finalità di maggiore leggibilità del MANUALE, gli Articoli con oggetti fra loro attinenti nell'ambito di ogni Sezione potranno essere raggruppati da un titolo comune che svolgerà dunque la funzione di capitolo pur non essendo necessario prevederne una codifica.

Gli Articoli possono fare riferimento a documenti allegati che verranno numerati progressivamente all'interno del testo. Successivamente al primo richiamo ad un allegato, lo stesso potrà essere citato da altri Articoli che trattino argomenti logicamente correlati ai contenuti già presenti nell'allegato stesso.

La struttura ed i contenuti in dettaglio del MANUALE sono riportati nello schema seguente:

SEZIONE I: Contenuti Generali	
Articolo 1	Finalità
Articolo 2	Ambito di applicazione
Articolo 3	Struttura del Manuale
Articolo 4	Infrastruttura tecnologica e applicativa
Articolo 5	Sigle e definizioni
Articolo 6	Modalità di comunicazione alla Comunità Amministrata
SEZIONE II: Contenuti Organizzativi	
Articolo 7	Obiettivi di adeguamento alla normativa
Articolo 8	Accreditamento dell'Amministrazione
Articolo 9	Area Organizzativa Omogenea
Servizio per la Tenuta del Protocollo Informatico della Gestione dei Flussi Documentali e degli Archivi (SPI)	
Articolo 10	Struttura e compiti di SPI
Articolo 11	Responsabile di SPI e suo vicario
Servizio Informativo Automatizzato (SIA)	
Articolo 12	Struttura e compiti del SIA
Articolo 13	Responsabile del SIA e suo vicario
Articolo 14	Compiti del SIA particolarmente rilevanti

Sicurezza dei Dati Personali	
Articolo 15	Responsabile della Sicurezza dei Dati Personali e suo vicario
Altre misure organizzative	
Articolo 16	Unità Organizzative Responsabili
Articolo 17	Modello organizzativo adottato nella gestione dei documenti
Articolo 18	Misure tecniche ed organizzative per l'eliminazione dei protocolli separati
SEZIONE III: Strumenti Archivistici	
Articolo 19	Quadro di classificazione
Articolo 20	Trasferimento dei documenti nell'archivio di deposito
Articolo 21	Trasferimento dei documenti nell'archivio storico
Articolo 22	Piano di conservazione dell'archivio
Articolo 23	Regolamentazione dell'accesso all'archivio
SEZIONE IV: Organizzazione della Gestione dei Documenti	
Articolo 24	Fasi rilevanti della gestione dei documenti
Articolo 25	Produzione
Articolo 26	Ricezione
Articolo 27	Protocollazione e classificazione
Articolo 28	Fascicolazione
Articolo 29	Spedizione
Articolo 30	Archiviazione e conservazione
SEZIONE V: Flussi di Lavorazione dei Documenti	
Articolo 31	Distribuzione con assegnazione dei documenti in arrivo
Articolo 32	Gestione integrata dei fascicoli, dei flussi documentali e dei procedimenti amministrativi
SEZIONE VI: Accessibilità e Sicurezza dei Documenti	
Articolo 33	Caratteristiche del Piano della Sicurezza dei Documenti Informatici
Articolo 34	Analisi dei rischi
Politiche di Sicurezza ed Interventi Operativi: Misure di Carattere Generale	
Articolo 35	Accesso fisico agli uffici di SPI, SIA e delle UOR
Articolo 36	Livelli di riservatezza
Articolo 37	Profili utente e autorizzazioni d'accesso
Articolo 38	Password
Articolo 39	Clear screen e clear desk policy
Articolo 40	Le stampe
Articolo 41	Protezione da software malizioso e da intrusioni esterne
Articolo 42	Salvataggio dei dati correnti
Articolo 43	Misure per la continuità del servizio
Articolo 44	Tracciamento delle operazioni
Politiche di Sicurezza ed Interventi Operativi: Misure di Sicurezza relative alle Fasi di Lavorazione	
Articolo 45	Produzione
Articolo 46	Ricezione
Articolo 47	Protocollazione e classificazione
Articolo 48	Fascicolazione
Articolo 49	Spedizione
Articolo 50	Archiviazione e conservazione
Articolo 51	Gestione dei flussi documentali
SEZIONE VII: Tempificazione	

Articolo 52	Prima fase di attuazione
Articolo 53	Seconda fase di attuazione.
ALLEGATI	
Allegato 1	Caratteristiche dell'Infrastruttura Tecnologica ed Applicativa.
Allegato 2	Struttura del Servizio per la tenuta del Protocollo Informatico, della Gestione dei Flussi Documentali e degli Archivi
Allegato 3	Caratteristiche delle Unità Organizzative Responsabili
Allegato 4	Titolario di classificazione
Allegato 5	Massimario di scarto degli atti d'archivio
Allegato 6	Analisi dei Rischi

Articolo 4: Infrastruttura tecnologica e applicativa

Come desumibile dal contenuto della Sez. VII, sono previste due fasi di attuazione distinte che richiedono diverse infrastrutture tecnologiche ed applicative che sono descritte nell'Allegato 1. L'Allegato riporta infatti sia le caratteristiche tecniche generali del sistema informatico preesistente alla costituzione di **SPI**, che l'indicazione dei tempi e delle modalità di attivazione delle infrastrutture tecnologiche ed applicative con le caratteristiche minime indispensabili per supportare anche parzialmente l'organizzazione del protocollo, degli archivi e dei flussi documentali previsti dal MANUALE nella prima fase di attuazione. Con il termine "caratteristiche minime" si intendono quelle che, in base all'Art. 3, comma 1, lett. d del DPCM 31 Ottobre 2000, consentono l'eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal DPR 428/1998

L'Allegato 1 indica inoltre, in funzione dei prevedibili impegni finanziari e degli eventuali vincoli tecnici od organizzativi, le caratteristiche ed i presumibili tempi di realizzazione delle infrastrutture tecnologiche e applicative necessarie per supportare in modo ottimale ed integrale l'intera organizzazione del protocollo, degli archivi e dei flussi documentali previsti dal MANUALE nella seconda fase di attuazione.

Successivamente o parallelamente, la disponibilità sul mercato di soluzioni tecnologiche ed applicative affidabili esterne all'Amministrazione (ad es. applicazioni informatiche con tipologia ASP) e fruibili dalla stessa con basso impegno finanziario e di infrastrutture, potrà condurre a scelte di innovazione del Sistema di gestione informatica dei documenti pur nel rispetto di tutte le misure di carattere organizzativo e di sicurezza previste dal MANUALE.

Richiamiamo che l'Art. 70 del DPR 445/2000 prescrive che le pubbliche amministrazioni devono assicurare, per ogni aggiornamento del sistema, il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti.

Pertanto, successivamente all'approvazione del MANUALE, l'Amministrazione si impegna, compatibilmente con le relative disponibilità finanziarie e gli accertati eventuali vincoli tecnici ed organizzativi, a definire, su indicazione del Responsabile del Servizio Archivistico di cui all'Art. 11 della Sez. II, la possibilità di recuperare e riutilizzare i dati preesistenti attinenti all'oggetto del MANUALE con modalità tecniche compatibili con gli strumenti informatici già a disposizione, con quelli che saranno disponibili in accordo al comma 1 del presente Articolo e con l'infrastruttura tecnologica che si intende adottare in accordo al comma 3 del presente Articolo.

Articolo 5: Sigle e definizioni

Di seguito sono riportate le definizioni dei termini ed il significato delle sigle abbreviate usate nel MANUALE.

SIGLE	SIGNIFICATO
SPI	Servizio per la tenuta del Protocollo Informatico, della gestione dei Flussi Documentali e degli Archivi (Servizio Archivistico)
AOO	Area Organizzativa Omogenea
UOR	Unità Organizzativa Responsabile
RSPI	Responsabile di SPI
SIA	Servizio Informativo Automatizzato
RSIA	Responsabile di SIA
RSDP	Responsabile della Sicurezza dei Dati Personali
RUOR	Responsabile di UOR
RPA	Responsabile del Procedimento Amministrativo
TERMINE	DEFINIZIONE
Amministrazione	Comune di BRUINO
Archivio corrente	L'insieme dei documenti amministrativi relativi a pratiche in corso o comunque per le quali sussiste un interesse corrente.
Archivio di deposito	L'insieme dei documenti relativi a pratiche concluse, ma non ancora destinate alla conservazione permanente ed alla consultazione pubblica.
Archivio storico	L'insieme dei documenti relativi a pratiche concluse destinato alla conservazione permanente e organizzato per garantirne la consultazione pubblica.
Area Organizzativa Omogenea	L'intera organizzazione dell'Amministrazione comprendente tutti gli uffici esistenti o che verranno istituiti, nessuno escluso.
Assegnazione	Individuazione della UOR competente per la trattazione della pratica o del procedimento amministrativo a cui un documento ricevuto dall'Amministrazione inerisce.
Casella Interna	Locazione logica prevista dal sistema di gestione informatica dei documenti a cui sono indirizzabili messaggi e documenti informatici destinati ad una UOR o a SPI . Per esigenze organizzative le Caselle Interne possono fare riferimento anche a singole strutture appartenenti a UOR o a SPI e a singoli responsabili o incaricati.
Documento Amministrativo	Rappresentazione, comunque formata, del contenuto di atti, anche interni, delle P.A. o, comunque utilizzati ai fini dell'attività amministrativa delle stesse.
Documento Informatico	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento Riservato	Documento amministrativo e/o informatico a cui è stato assegnato un livello di riservatezza medio o alto.
Fascicolazione	Individuazione del fascicolo di competenza di un singolo documento amministrativo od informatico e posizionamento dello stesso in suo riferimento al suo interno.
Fascicolo	Unità archivistica che comprende tutti i documenti amministrativi od informatici relativi ad una pratica o ad un procedimento

	amministrativo.
Firma digitale	Risultato della procedura informatica di validazione basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore tramite la chiave privata ed al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e la integrità di un documento informatico o di un insieme di documenti informatici.
Funzionalità applicative	Qualsiasi attività specifica anche di dettaglio relativa alla gestione dei documenti, prevista o meno espressamente dal manuale di gestione, comunque supportata da procedure informatiche e da programmi applicativi o da componenti di essi.
Gestione dei documenti	L'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi di gestione informatica dei documenti.
Impronta del documento informatico	Sequenza di simboli binari che identificano univocamente l'integrità di un documento informatico. Essa viene calcolata, attribuita e crittografata dal procedimento di firma digitale con validità legale o meno.
Indice di classificazione	Sequenza di codici identificativi degli elementi gerarchici previsti dalla struttura del Titolare di classificazione. Ad es. titolo – classe - sottoclasse. Il codice del fascicolo non è compreso nell'indice.
Informazione Riservata	Qualsiasi informazione contenuta od inerente ad un documento riservato che costituisca elemento specifico dello stesso.
Infrastruttura tecnologica ed applicativa	Insieme delle risorse di elaborazione (centrali e periferiche), degli apparati, reti di comunicazione, software di base e d'ambiente e procedure informatiche di gestione dei dati utilizzato dall'Amministrazione per realizzare la gestione dei documenti.
Personale addetto	Qualsiasi unità di personale appartenente alla AOO che svolge continuativamente o è chiamato a svolgere anche episodicamente, attività inerenti alla gestione dei documenti.
Piano di conservazione degli archivi	Piano rappresentativo dei criteri di organizzazione degli archivi in accordo al sistema di classificazione che disciplina le attività di selezione e di scarto al fine ultimo di garantire la conservazione permanente dei documenti nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali.
Scansione ottica	Operazione tecnica atta a produrre un documento informatico in formato immagine a partire da un documento cartaceo.
Segnatura di protocollo	Associazione o apposizione all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti l'operazione di registrazione di protocollo del documento stesso.
Sistema di gestione informatica dei documenti	L'insieme della infrastruttura tecnologica ed applicativa, degli archivi corrente, di deposito e storico memorizzati su supporto di memorizzazione fisso o removibile, delle regole di gestione dei documenti e del software applicativo di gestione degli stessi.
Titolario di classificazione	Sistema gerarchico predefinito di partizioni, individuate in accordo alle competenze e ambiti di attività dell'Amministrazione, al quale devono riferirsi tutti i documenti amministrativi trattati, al fine di organizzarli logicamente in modo da rispecchiare l'evoluzione storica delle attività svolte. La struttura del titolare di classificazione

	definisce univocamente la struttura dell'indice di classificazione.
Unità Organizzativa Responsabile	Ufficio o raggruppamento di uffici a cui sono attribuite le responsabilità di gestione dei documenti previste dal manuale ed inerenti ai propri compiti all'interno della AOO che realizza tramite proprie risorse autonome umane e materiali.

Articolo 6: Modalità di comunicazione alla Comunità Amministrata

Il presente Manuale, in base a quanto indicato nelle Linee Guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi del 14/10/03, viene pubblicato e reso accessibile tramite il sito Internet di questo Comune.

SEZIONE II: Contenuti Organizzativi

Articolo 7: Obiettivi di adeguamento alla normativa

Al fine di conseguire gli obiettivi delle Pubbliche Amministrazioni di adeguamento alla normativa del Protocollo Informatico in accordo all'Art. 3, comma 1, lett. a,b,c del DPCM 31 Ottobre 2000, l'Amministrazione ha:

- individuato l'intera organizzazione comunale come singola ed unica Area Organizzativa Omogenea ai sensi dell'art. 2 del DPR 428/1998. I relativi uffici di riferimento sono dunque tutti gli uffici del Comune nessuno escluso. Le informazioni di dettaglio sulla **AOO** previste all'art. 12 comma 2 del DPCM 31 Ottobre 2000 sono riportate all'Art. 9 della Sez. II;
- ha provveduto a costituire il Servizio per la tenuta del Protocollo Informatico, della Gestione dei Flussi Documentali e degli Archivi (**SPI**, altrimenti definito come Servizio Archivistico) in base all'art. 61 del DPR 445/2000. I compiti assegnati al servizio sono indicati nell'Art. 10 della Sez. II;
- ha nominato il Responsabile di **SPI** con gli obiettivi ed i compiti previsti all'art. 5, comma 1, lett. a,b,c del DPCM 31 Ottobre 2000, di seguito denominato **RSPI**, come indicato nell'Art. 11 della Sez. II;
- ha adottato su proposta di **RSPI** il presente Manuale di Gestione dei Documenti redatto in accordo all'Art. 5 del DPCM 31 Ottobre 2000.

Articolo 8: Accredimento dell'Amministrazione

L'Amministrazione ha provveduto ad accreditarsi presso l'Indice delle Amministrazioni Pubbliche e delle Aree Organizzative Omogenee previsto dall'Art. 11 del DPCM 31 Ottobre 2000 fornendo le seguenti informazioni:

- Denominazione della Amministrazione: **COMUNE DI BRUINO**
- Codice identificativo proposto per la Amministrazione: **COMUNE DI BRUINO**
- Indirizzo della sede principale della Amministrazione: **P.ZA MUNICIPIO 3**
- L'unica Area Organizzativa Omogenea è: **COMUNE DI BRUINO**

Articolo 9: Area Organizzativa Omogenea

La **AOO** a cui si riferisce il MANUALE è il Comune di **BRUINO** di cui, in accordo all'Art. 12 del DPCM 31 Ottobre 2000, si riportano le seguenti informazioni:

- Denominazione: **COMUNE DI BRUINO**
- Codice identificativo: **COMUNE DI BRUINO**
- Casella di Posta Elettronica Istituzionale dell'Area: **comune@comune.bruino.to.it**
- Il nominativo del responsabile del Servizio per la tenuta del Protocollo Informatico, per la Gestione dei Flussi Documentali e degli Archivi è riportato nell'Allegato 2.
- Data di istituzione: **01/01/2004**
- L'elenco degli uffici utenti che compongono l'Area è riportato nell'Allegato 3.

Servizio per la Tenuta del Protocollo Informatico, della Gestione dei Flussi Documentali e degli Archivi (SPI)

Articolo 10: Struttura e compiti di SPI

Nell'Allegato 2 è indicata la dotazione organica di **SPI**. Nello stesso allegato sono indicati i ruoli degli addetti in riferimento ai contenuti e alle attività disciplinate dal MANUALE.

SPI svolge i seguenti compiti istituzionali:

- attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione e segnatura di protocollo si svolgano nel rispetto delle disposizioni del testo unico 445/2000;
- garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'art. 53 del DPR 445/2000;
- cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro 24 ore di blocco delle attività e, comunque, nel più breve tempo possibile;
- conserva le copie di cui agli art. 62 e 63 del DPR 445/2000 (procedure di salvataggio e conservazione, registro di emergenza), in luoghi sicuri e differenti;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione della attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli art. 59 e 60 del DPR 445/2000 (accesso esterno e accesso effettuato dalle P.A.) e le attività di gestione degli archivi di cui agli art. 67, 68 e 69 del DPR 445/2000 (trasferimento all'archivio di deposito, disposizioni per la conservazione degli archivi, archivi storici);
- autorizza le operazioni di annullamento di cui all'art. 54 del DPR 445/2000;
- vigila sull'osservanza delle disposizioni del DPR 445/2000 da parte del personale autorizzato e degli incaricati.

Inoltre, il servizio svolge i seguenti compiti particolari attinenti allo specifico modello organizzativo adottato dall'Amministrazione e descritto in dettaglio dal MANUALE:

- vigila sull'osservanza delle disposizioni del MANUALE da parte del personale. In particolare sarà compito di **SPI** vigilare in merito ai trattamenti effettuati da parte delle **UOR** sui documenti informatici prodotti a fine di garantirne l'integrità e la riservatezza (firma digitale e crittografia);
- svolge un ruolo di consulenza nei confronti del personale delle **UOR** che espleta attività inerenti o correlate alla protocollazione, alla gestione degli archivi e dei flussi documentali;
- svolge compiti di supervisione sulle attività delle **UOR** inerenti alla protocollazione, alla gestione degli archivi e dei flussi documentali. In particolare effettua periodicamente controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale, e sull'utilizzo di un unico registro informatico, verificando, attraverso specifici controlli mirati sull'operato delle **UOR**, la correttezza delle operazioni di classificazione e di fascicolazione archivistica.

Articolo 11: Responsabile di SPI e suo vicario

L'Amministrazione ha nominato il Responsabile di **SPI** in base ad una valutazione di possesso di idonei requisiti professionali per ricoprire il ruolo. Eventuali necessità future di maggiori competenze sia tecnico archivistiche che di tipologia diversa comunque attinenti, saranno conseguibili tramite processi di formazione definiti secondo le procedure descritte dalla disciplina vigente di cui si fa menzione nell'Allegato 2 ove sono descritte le modalità di Formazione Permanente di **RSPI**.

Su proposta di **RSPI**, l'Amministrazione ha nominato il suo vicario per casi di vacanza, assenza o impedimento.

I nominativi di **RSPI** e del suo vicario sono riportati nell'Allegato 2.

E' compito di **RSPI** identificare, nell'ambito del personale assegnato a **SPI**, i soggetti destinati a svolgere i compiti istituzionali o particolari elencati nell'Art. 10 della Sez. II. Di tale identificazione viene riportata menzione nell'ambito dell'Allegato 2.

Servizio Informativo Automatizzato (SIA)

Articolo 12: Struttura e compiti del SIA

Nella dotazione organica di questo Ente non è attualmente prevista la figura di un Esperto Informatico o equivalente. Per sopperire a tali funzioni ci si avvale di un consulente esterno dipendente di altro Ente.

I suoi compiti operativi consistono nell'assicurare il regolare funzionamento dell'apparato informatico, atto a gestire il regolare svolgimento del flusso documentale e le opportune misure di protezione e conservazione dei dati del Protocollo informatico.

Provvede altresì a ripristinare entro 24 ore e comunque nel più breve tempo possibile le funzionalità del sistema in caso di interruzioni o anomalie.

Articolo 13: Responsabile del SIA e suo vicario

In mancanza di Esperto Informatico in dotazione organica, le figure di Responsabile di SIA di seguito indicato con la sigla **RSIA** e suo vicario coincidono con i soggetti nominati Responsabile di SPI e vicario di seguito indicati con la sigla **RSPI**.

Il **RSIA** costituisce pertanto l'interlocutore amministrativo interno del consulente informatico di cui l'amministrazione si avvale e ne acquisisce i pareri facendoli propri.

Articolo 14: Compiti del SIA particolarmente rilevanti

Oltre ai compiti descritti nel precedente articolo, il **SIA** svolge i compiti che si giudicano pertinenti e rilevanti per il raggiungimento degli obiettivi che l'Amministrazione si pone con l'attuazione della normativa sulla tenuta del Protocollo Informatico, della Gestione degli Archivi e dei Flussi Documentali.

Sicurezza dei Dati Personali

Articolo 15: Responsabile della Sicurezza dei Dati Personali e suo vicario

Le figure di Responsabile della Sicurezza dei Dati Personali e suo vicario di seguito indicati con la sigla **RSDP** coincidono con i soggetti nominati Responsabile di SPI e vicario di seguito indicati con la sigla **RSPI**.

RSDP ha il compito di:

- vigilare sull'osservanza delle disposizioni previste dal regolamento di attuazione emanato con DPR 28 luglio 1999, n° 318, in attuazione dell'art. 15 comma 2 della legge 675/1996 ora D.Lgs. 196/03 da parte del personale nella gestione dei documenti;
- vigilare sull'osservanza delle disposizioni del MANUALE riguardanti la sicurezza dei documenti contenenti dati personali o dati sensibili da parte del personale;
- adeguare il MANUALE in riferimento all'applicazione del DL 196 del 30 Giugno 2003.

Altre Misure Organizzative

Articolo 16: Unità Organizzative Responsabili

Oltre al già citato elenco delle **UOR**, l'Allegato 3 riporta per ogni unità afferente alla **AOO** le seguenti informazioni:

- denominazione della **UOR**;
- nominativo del Responsabile della **UOR**, di seguito indicato con la sigla **RUOR**;
- elenco degli uffici afferenti alla **UOR**;

E' compito di **RUOR** organizzare le attività di produzione dei documenti in modo tale da garantire, anche in fase di preparazione degli stessi, opportuni criteri di disponibilità, integrità e riservatezza delle bozze e di qualsiasi componente documentale intermedia funzionale alla fase preparatoria dei documenti stessi. A tale scopo sarà compito di **RUOR** disciplinare le attività di salvataggio periodico (backup) dei contenuti delle memorie di massa delle stazioni di lavoro utilizzate, dell'apposizione della firma digitale senza validità legale e della eventuale crittografia ai documenti in preparazione in modo da garantirne l'integrità e la riservatezza.

Articolo 17: Modello organizzativo adottato nella gestione dei documenti

Il Modello organizzativo adottato nella gestione dei documenti è del tipo distribuito. Il modello prevede che **SPI** esegua in modo esclusivo le fasi di ricezione, classificazione e protocollazione dei documenti in arrivo.

Per documenti in arrivo si intendono quelli che hanno rilevanza giuridico - probatoria, acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni.

Per particolari esigenze organizzative, alcune di queste funzioni possono anche essere svolte da personale delle **UOR** che, solo per queste funzioni, dipenderà comunque da **SPI**. Compito della **UOR** è quello di partecipare attivamente alla formazione dell'archivio registrando autonomamente i documenti in partenza da essa prodotti e curando la formazione dei fascicoli e la gestione dei flussi documentali anche per ciò che riguarda i documenti in arrivo di propria competenza.

Per documenti in partenza si intendono i documenti che hanno rilevanza giuridico - probatoria prodotti dal personale dell'Amministrazione nell'esercizio delle proprie funzioni. Definiamo inoltre come interni i documenti scambiati tra le diverse **UOR** distinguibili in:

- documenti di preminente carattere informativo;
- documenti di preminente carattere giuridico - probatorio.

ed omettiamo i documenti interni scambiati tra **UOR** ed organi che non vanno considerati di interesse per gli scopi del MANUALE.

La protocollazione dei documenti in partenza è svolta dunque direttamente dalle unità che producono gli atti, che ne effettuano la classificazione, la fascicolazione e la spedizione. A questo riguardo l'Art. 10 della Sez. II prevede che **SPI** svolga anche compiti di supporto e di supervisione sulle attività delle **UOR** inerenti sia la protocollazione in partenza che la gestione dei flussi documentali.

I dettagli delle fasi di gestione dei documenti previste dal modello organizzativo adottato sono descritti nella Sez. IV e, per quanto riguarda la sicurezza dei documenti, nella Sez. V.

Articolo 18: Misure tecniche ed organizzative per l'eliminazione dei protocolli separati

Nell'ambito di questo Comune non vi sono protocolli interni da eliminare (art. 3, comma 1, lett. d) DPCM 31/10/2000.

SEZIONE III: Strumenti Archivistici

Articolo 19: Quadro di classificazione

Nell'Allegato 4 viene riportato il quadro di classificazione dei documenti (Titolario di archivio) con i relativi indici: sistematico e alfabetico.

Articolo 20: Trasferimento dei documenti nell'archivio di deposito

SPI provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso la **AOO**.

Nell'Art. 30 della Sez. IV sono definiti i criteri e la tempistica dell'aggiornamento (almeno una volta l'anno: Art 67 comma 1 DPR 445/2000) da parte di **SPI** dell'archivio di deposito su indicazione delle **UOR** competenti. L'archivio comunque centralizzato è accessibile senza necessità di autorizzazione da parte delle **UOR** per le pratiche di propria competenza e, previa autorizzazione di **RSPI**, per le pratiche di specifico interesse documentato.

Articolo 21: Trasferimento dei documenti nell'archivio storico

I documenti selezionati per la conservazione permanente sono trasferiti, contestualmente agli strumenti che ne garantiscono l'accesso, nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei Beni Culturali. Nell'Allegato 5, viene riportato il massimario di selezione e scarto.

Articolo 22: Piano di conservazione dell'archivio

L'Archivio del Comune di Bruino è costituito dal complesso dei documenti prodotti e acquisiti dall'Ente nello svolgimento della propria attività e nell'esercizio delle proprie funzioni. Esso comprende anche i fondi archivistici di enti e istituti cessati, le cui funzioni e/o proprietà sono state trasferite al Comune.

L'Archivio si divide in :

- 1.archivio corrente
- 2.archivio di deposito
- 3.archivio storico

L'Archivio corrente è costituito dall'insieme dei documenti relativi ai procedimenti amministrativi non ancora conclusi. Ciascun servizio comunale gestisce ed organizza i documenti di propria competenza, mantenendo i propri archivi secondo autonome regole interne autodefinite.

L'Archivio di deposito è costituito dalla documentazione riferita a procedimenti amministrativi che, sebbene conclusi, possono essere riassunti in esame o per

un'eventuale ripresa o per un interesse sporadico legato all'analogia o alla connessione con pratiche successive.

L'Archivio di deposito raccoglie, ordina, seleziona ai fini della conservazione permanente e rende consultabile nel rispetto delle leggi vigenti tutta la documentazione di valore archivistico che, non essendo più strettamente necessaria per il disbrigo dei procedimenti correnti non è, tuttavia, ancora nelle condizioni di essere collocata, a norma di legge (cioè trascorsi quarant'anni dalla conclusione della pratica), presso l'archivio storico.

L'operazione di riordino dell'archivio viene fatta di norma con scadenza annuale e consiste nella schedatura delle carte, organizzazione delle schede, creazione di elenchi di materiale omogeneo, aggiornamento degli strumenti di consultazione, sistemazione fisica del materiale attraverso il nuovo titolario di classificazione (Allegato 4). L'aggiornamento del titolario compete esclusivamente al Responsabile SPI ed è assicurato quando se ne presenta la necessità, nel pieno rispetto delle disposizioni contenute nella normativa vigente in materia di formazione e conservazione degli archivi. Dopo ogni modifica del titolario, il Responsabile SPI provvede a informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare le istruzioni per il corretto utilizzo delle nuove classifiche. Nell'ambito dell'archivio di deposito vengono effettuate le operazioni di selezione e scarto. I documenti selezionati per l'eliminazione vengono descritti in un elenco contenente i riferimenti alle categorie del titolario di classificazione, il numero e la tipologia delle unità archivistiche, gli estremi cronologici, la descrizione della documentazione. Tale elenco, sotto forma di proposta di scarto costituente oggetto di una determinazione del Funzionario del Settore Affari Generali, viene trasmesso alla Soprintendenza archivistica per il rilascio del nulla osta alla eliminazione. Ottenuto il nulla osta è possibile conferire il materiale alla Croce Rossa per la distruzione.

Le operazioni di selezione e scarto sono sempre preliminari al passaggio della documentazione all'archivio storico.

L'Archivio storico, riordinato nell'anno 1997 con contributo regionale a cura di archivisti segnalati dalla Soprintendenza Archivistica, è costituito dai documenti relativi a procedimenti amministrativi esauriti da oltre quarant'anni che coprono un periodo di tempo dal 1616 al 1959. I documenti dell'archivio storico sono destinati alla conservazione permanente per finalità di tipo prevalentemente storico-culturale e di ricerca.

Archivio di deposito e Archivio storico sono conservati in modo distinto presso il locale destinato all'Archivio Comunale, sito al piano terra, all'interno del Palazzo comunale. Tali locali, ristrutturati recentemente, rispondono alle norme di sicurezza e antincendio richiesti dalla legge. Gli arredi sono composti da armadi e scaffali metallici che offrono le opportune garanzie contro gli incendi e l'assorbimento della polvere.

Articolo 23: Regolamentazione dell'accesso all'archivio

Ai sensi del Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi approvato da questa Amministrazione in data 25.11.1997 e successive integrazioni i documenti appartenenti all'archivio possono essere consultati, nel rispetto della legge sulla privacy, con la presenza di personale addetto che è tenuto a fornire la necessaria assistenza.

E' vietato asportare i documenti dal luogo presso cui sono dati in visione, tracciare segni su di essi o comunque alterarli in qualsiasi modo. L'esame dei documenti è gratuito. L'interessato può prendere appunti e trascrivere in tutto o in parte i documenti presi in visione ed è responsabile degli eventuali danni ad essi arrecati. I documenti possono essere fotocopiati (solamente se da tale operazione non derivi danno al documento stesso) a cura del personale addetto dietro pagamento del relativo rimborso spese previsto dall'apposito regolamento

SEZIONE IV: Organizzazione della Gestione dei Documenti

Articolo 24: Fasi rilevanti della gestione dei documenti

Come già accennato nell'Art. 2 della Sez. I, il MANUALE non si pone come obiettivo di disciplinare l'iter dei procedimenti amministrativi e quindi non tratterà nessuna delle fasi di gestione della produzione dei documenti né la circolazione interna dei documenti fra **UOR**. I **RUOR** garantiranno che i trattamenti documentali effettuati nell'ambito delle **UOR**, al fine di giungere alla formulazione del documento nella sua versione definitiva, dovranno essere comunque gestiti con modalità in accordo ai principi di garanzia della Sicurezza delle Informazioni e di Protezione dei Dati Personali previsti dalla Sez. VI.

Le fasi che verranno tenute in considerazione dal MANUALE saranno dunque le seguenti:

- **Produzione** (solo dal momento della presa in carico o della redazione del documento definitivo da parte del Responsabile del Procedimento Amministrativo di seguito denominato **RPA**).
- **Ricezione**.
- **Protocollazione e Classificazione**: fase successiva alla produzione per i documenti in partenza o alla ricezione per i documenti in arrivo.
- **Fascicolazione**: fase successiva alla protocollazione e classificazione per tutti i tipi di documento.
- **Spedizione**: fase successiva alla fascicolazione per documenti in partenza.
- **Archiviazione e Conservazione**: fase successiva alla fascicolazione per tutti i tipi di documento.

Le attività connesse ad ognuna delle fasi sopra elencate trovano una loro sintetica descrizione nei successivi articoli della presente Sezione ove vengono anche riportate le istruzioni per la loro corretta esecuzione. Ulteriori istruzioni riguardanti in particolare la sicurezza dei documenti nelle diverse fasi della gestione, sono riportate nella Sez. V.

Ognuna delle fasi sopraindicate e di seguito dettagliatamente descritte in termini di singole attività, vanno considerate realizzate con il supporto di una opportuna infrastruttura tecnologica ed applicativa che potrà realizzare con modalità controllata tutte o in parte le funzionalità previste. Anche in caso di tempi di adeguamento dell'infrastruttura tecnologica ed applicativa (Allegato 1) più lunghi di quelli di adozione e operatività del MANUALE indicati nella Sez. VII, ciò avrà come effetto solo quello di comportare la necessità di gestire manualmente eventuali controlli, passaggi fra fasi, verifiche di congruenza fra dati e documenti, ecc. E' comunque escluso che ritardi nell'implementazione di un sistema informatico di gestione integrata dei documenti possa mettere in discussione le regole, le misure, i comportamenti, le responsabilità e quanto d'altro previsto dal MANUALE al fine di rendere operativo il modello di gestione documentale adottato.

In altri termini, ciò significa che all'interno del MANUALE non troveranno posto considerazioni relative alla gestione del protocollo, archivi e flussi documentali effettuata manualmente in riferimento esclusivamente a documenti cartacei.

Articolo 25: Produzione

La produzione dei documenti è una attività di competenza esclusiva delle **UOR**. Quando si produce un documento è consigliabile utilizzare, a partire dalla versione in bozza, strumenti informatici di produttività individuale al fine di poter generare un documento informatico al quale è possibile apporre la firma digitale. In caso di produzione di un documento in originale necessariamente cartaceo, ad esempio derivante da compilazione di prestampato o altri casi analoghi, esso va comunque assoggettato a scansione ottica e successivamente sottoscritto con firma digitale. Il presupposto del modello organizzativo adottato nel MANUALE è che tutte le **UOR** siano in grado di produrre solo documenti informatici resi imm modificabili con firma digitale con valore legale o meno.

Nella produzione dei documenti oggetto di protocollazione devono essere previsti e definiti almeno i seguenti attributi:

- denominazione dell'Amministrazione;
- logo dell'Amministrazione;
- indicazione della **UOR** che ha prodotto il documento;
- indirizzo completo della **AOO** (via, numero, c.a.p., città, provincia);
- numero telefonico;
- numero di telefax;
- indirizzo istituzionale di posta elettronica;
- data completa (luogo, giorno, mese, anno) scritta per esteso;
- anno e numero di protocollo;
- indice di classificazione completato dal numero di fascicolo;
- numero degli allegati se presenti;
- descrizione degli allegati se presenti;
- oggetto del documento;
- firma autografa o digitale di **RPA** quale sottoscrittore;
- nome e cognome del sottoscrittore;
- qualifica rivestita dal sottoscrittore.

Il documento formato dall'istruttore va inviato a **RPA** che:

- prende in carico il documento prodotto nella sua versione definitiva già in formato elettronico;
- verifica la presenza e la completezza della definizione degli attributi previsti e può riservarsi di compilarne alcuni non ancora definiti;
- appone la firma digitale con validità legale quando prevista altrimenti lo rende comunque non modificabile tramite l'applicazione della firma digitale senza validità legale;
- assegna il livello di riservatezza che ritiene più opportuno in funzione della tipologia, dei contenuti e delle caratteristiche di riservatezza del fascicolo a cui sarà attribuito;
- se il documento è destinato ad essere spedito per via telematica, lo inoltra alla Casella di Posta Elettronica Istituzionale da cui deve essere spedito;
- se il documento è destinato ad essere spedito in formato cartaceo, viene stampato e firmato in copia cartacea originale;
- il documento informatico passa alla fase di fascicolazione descritta nell'Art. 28 della Sez. IV.

Consideriamo che ogni documento cartaceo in partenza o interno doveva di norma essere redatto in due esemplari, cioè in originale e in minuta. Per originale si intendeva il documento nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali, mentre per minuta si intendeva l'originale del documento conservato "agli atti", cioè nel fascicolo relativo alla pratica o al procedimento amministrativo trattato.

Nel caso di documento informatico spedito con strumenti telematici l'esemplare oggetto di spedizione e quello archiviato debbono essere identici.

Viceversa, nel caso di documento informatico spedito in formato cartaceo, l'esemplare cartaceo deve essere prodotto dal sottoscrittore e solo da esso con opportuna operazione di stampa solo successivamente alla redazione del documento informatico definitivo completo di firma digitale senza valore legale. L'originale prodotto dalla funzione di stampa e destinato alla spedizione, va sottoscritto con firma autografa, mentre il documento informatico viene archiviato nel sistema di gestione informatica dei documenti.

Articolo 26: Ricezione

La ricezione dei documenti è una attività di competenza esclusiva di **SPI**.

La posta rilevante ai fini del protocollo comunque giunta agli indirizzi dell'Amministrazione tramite:

- il servizio postale tradizionale;
- la consegna diretta agli uffici dell'Amministrazione;
- gli apparecchi telefax;

va inviata a **SPI** corredata da timbro datario nel più breve tempo possibile. I documenti inviati dal mittente per Posta Elettronica devono comunque essere ricevuti direttamente sulla Casella di Posta Elettronica Istituzionale. E' esclusa la possibilità che documenti ricevuti ad indirizzi di posta elettronica diversi da quello ufficiale siano inoltrati a cura del addetti alla Casella di Posta Elettronica Istituzionale, tali documenti vengono trattati come documenti personali e quindi non soggetti a protocollazione. Come tali resta esclusiva responsabilità del destinatario della e-mail, comunicare al mittente l'eventuale errore di indirizzo elettronico e, contestualmente, indicare l'indirizzo corretto della Casella di Posta Elettronica Istituzionale.

In caso di documenti cartacei solo le lettere recanti sull'esterno della busta l'indicazione di **RISERVATA PERSONALE** vengono consegnate al destinatario in indirizzo e sono escluse dalla protocollazione.

Nel caso di documenti consegnati a mano (ad es. agli sportelli), va rilasciata ricevuta.

Attività inerenti la ricezione dei documenti:

- **In caso di documenti in formato cartaceo, SPI:**
 - riceve e, quando non esistono motivi particolari ad es. offerte in risposta a gare, apre la posta;
 - assegna al documento il livello di riservatezza che ritiene più opportuno in funzione della tipologia di documento e dei suoi contenuti.

- **In caso di documenti in formato elettronico, SPI:**
 - riceve i documenti informatici sulla Casella di Posta Elettronica Istituzionale;
 - verifica la correttezza della ricezione;
 - in caso di giudizio negativo, notifica al mittente una segnalazione di errore;
 - in caso di risultato positivo provvede a verificarne la conformità:
 - in caso di giudizio positivo, inoltra il documento alla Casella Interna di **SPI** con l'attributo di "in fase di protocollazione";
 - in caso di giudizio negativo o di dubbio in merito alla conformità del documento, individua la **UOR** competente e verifica, tramite la procedura di "preassegnazione" descritta nel seguito, l'accettabilità dello stesso;
 - in caso di giudizio positivo, inoltra il documento alla Casella Interna di **SPI** con l'attributo di "in fase di protocollazione";
 - in caso di giudizio negativo, attiva il "rifiuto" in base alla procedura descritta nel seguito.

Livelli di riservatezza

Forme particolari di riservatezza debbono essere gestite per le seguenti tipologie di documenti:

- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo di competenza del Sindaco che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente (in particolare dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352 e dalla serie di norme collegate al D.Lgs 30 giugno 2003 n. 196);
- altri documenti che per ragioni strettamente legate a condizioni particolari dell'Amministrazione o del mittente sono da considerarsi in situazione analoga alle tipologie di documenti descritti nei punti precedenti.

Per garantire la particolare riservatezza a cui vanno assoggettati i documenti, si definisce un livello di riservatezza (Art. 36 della Sez. VI) suscettibile di assumere valori numerici interi da 1 a 3 corrispondenti a riservatezza bassa, media e alta.

Procedura di "preassegnazione" per la verifica di accettabilità del documento

I documenti informatici in arrivo privi di firma elettronica, con firma elettronica non conforme o comunque giudicati "non conformi" da **SPI** necessitano di decisioni da prendere caso per caso in merito alla loro accettabilità da parte dell'Amministrazione.

A tale scopo **SPI** procede come di seguito indicato:

- appone la firma digitale senza valore legale al documento sotto valutazione per garantirne l'integrità nel corso del processo;
- assegna al documento il livello di riservatezza che ritiene più opportuno in funzione della tipologia di documento e dei suoi contenuti;
- inoltra il documento alla Casella Interna di **SPI** con l'attributo di "in fase di verifica di accettabilità";
- inoltra il documento dalla Casella Interna di **SPI** alla Casella Interna di **RUOR** che si valuta competente in merito con l'indicazione delle non conformità e la richiesta di esprimersi in merito alla sua accettabilità:
 - se **RUOR** valuta non corretta la "preassegnazione", rispedisce il documento a **SPI** munito delle eventuali osservazioni di merito; ad esempio le eventuali informazioni in suo possesso per coadiuvare **SPI** nel successivo tentativo di "preassegnazione". La spedizione avviene con ricevuta di ritorno utilizzata da **RUOR** per cancellare il documento dalla propria Casella Interna. Anche in caso di errata "preassegnazione", il **RUOR** destinatario è comunque vincolato al trattamento del documento nel rispetto del livello di riservatezza attribuito da **SPI**. Seguirà da parte di **SPI** l'identificazione di altra **UOR** competente a cui indirizzare la "preassegnazione";
 - se **RUOR** valuta corretta la "preassegnazione" verifica il contenuto del documento e decide se accettarlo:
 - in caso di decisione positiva rispedisce il documento a **SPI** comunicandone la motivazione. La spedizione avviene con ricevuta di ritorno utilizzata da **RUOR** per cancellare il documento dalla propria Casella Interna. Rispedire a **SPI** il documento è necessario perché prima dell'assegnazione vera e propria, **SPI** deve effettuare le fasi di protocollazione e classificazione. In caso contrario **RUOR** sarebbe in possesso di un documento virtualmente assegnato e privo degli elementi indispensabili alla presa in carico;
 - in caso di decisione negativa rispedisce il documento a **SPI** comunicandone la motivazione e specificando se è opportuno notificare il rifiuto al mittente e la motivazione da adottare. La spedizione avviene con ricevuta di ritorno utilizzata da **RUOR** per cancellare il documento dalla propria Casella Interna.

In tutti i casi in cui, a giudizio esclusivo di **RSPI**, seguire la corretta procedura di pre-assegnazione (procedura standard) sopra indicata comporterebbe ritardi tali da pregiudicare il rispetto dei tempi richiesti dall'oggetto del documento, si può procedere con la modalità alternativa (procedura veloce) descritta nel seguito:

- **RSPI** individua il **RUOR** competente contattandolo verbalmente descrivendogli il documento;
- **RUOR** provvede eventualmente a visionare il documento in oggetto direttamente presso la sede di **SPI**;
- **RUOR** provvede a fornire le stesse informazioni previste in chiusura della procedura di pre-assegnazione in una forma concordata con **RSPI**;
- **RSPI** fornisce sotto la sua responsabilità le istruzioni agli addetti di **SPI** su come trattare il documento in oggetto.

La precedente procedura veloce per essere alternativa alla procedura di pre-assegnazione deve in ogni modo condurre al reperimento delle stesse informazioni che fornirebbe la procedura standard.

Procedura di rifiuto

A seguito della procedura di “preassegnazione” ed in caso di valutazione negativa da parte di **RUOR** competente in merito all'accettabilità di un documento informatico non conforme, si attiva la procedura di rifiuto descritta qui di seguito.

A seconda che **RUOR** competente definisca la necessità di notificare il rifiuto o meno di un documento informatico, **SPI** procede nel modo seguente:

- in caso di decisione da parte di **RUOR** competente di non notificare il rifiuto del documento informatico, **SPI** provvede a cancellare il messaggio in arrivo sulla Casella Istituzionale ed a cancellarlo dalla Casella Interna di **SPI** da cui è transitato nella fase di “preassegnazione”;
- in caso di decisione da parte di **RUOR** competente di notificare il rifiuto del documento informatico, **SPI** provvederà ad inviare un messaggio di risposta al messaggio originale del mittente con allegato il documento reso immodificabile tramite firma digitale senza valore legale (vedi procedura di “preassegnazione”) e testo del messaggio contenente l'indicazione dell'iter seguito nell'esame del documento e la motivazione per cui si è ritenuto di non considerarlo accettabile. Se il contenuto del documento suggerisce che lo stesso necessita di essere garantito in termini di riservatezza è opportuno comunicare al mittente le misure che sono state adottate in tal senso.

Articolo 27: Protocollo e classificazione

La protocollazione e classificazione per ciò che riguarda i documenti in arrivo è una attività di competenza esclusiva di **SPI**, mentre per ciò che riguarda i documenti in partenza è una attività di competenza esclusiva delle **UOR**.

In questa fase della gestione i documenti vengono:

- protocollati (attività di registrazione e di segnatura);
- classificati (in base al Titolario d'Archivio: Art. 20 della Sez. III);
- i documenti in arrivo in formato cartaceo vengono assoggettati a scansione ottica e resi immodificabili tramite l'apposizione della firma digitale con o senza validità legale in funzione del giudizio autonomo di **RSPI**. Tali documenti saranno trattati nel seguito come documenti informatici conformi a pieno titolo. Gli originali cartacei saranno immagazzinati in appositi magazzino con accesso riservato a **RSPI** e necessiteranno solo di essere repertoriati con l'indicazione del numero e anno di protocollo. Nel caso di documenti relativi a gare d'appalto che verranno assegnati e distribuiti in busta chiusa non verrà effettuata alcuna scansione ottica. La scansione ottica di questi ultimi documenti verrà effettuata solo al termine della gara quando saranno riconsegnati a questo scopo da **RUOR** a **SPI**;
- i documenti in partenza che non è possibile produrre in formato elettronico e quindi sono destinati necessariamente alla spedizione in formato cartaceo, vengono assoggettati a scansione ottica e sottoscritti con firma digitale senza validità legale.

Registrazione

I documenti da protocollare sono quelli dai quali possano nascere diritti, doveri o legittime aspettative di terzi. Il protocollo serve, infatti, ad attribuire ad un determinato documento data, forma e provenienza certa attraverso la registrazione dei seguenti elementi rilevanti sul piano giuridico – probatorio:

- data di registrazione;
- numero di protocollo;
- mittente per il documento in arrivo; destinatario per il documento in partenza;
- oggetto comprensivo di una breve descrizione degli elementi essenziali del contenuto del documento. L'oggetto va formulato tenendo in debito conto la necessità di non fornire informazioni riservate;
- indice di classificazione;
- numero degli allegati se presenti;

L'insieme dei suddetti elementi è denominata: «**Registrazione**».

Il sistema deve prevedere anche la registrazione, se trattasi di documento in arrivo e se disponibili, dei seguenti elementi:

- data del documento;
- numero di protocollo del documento.

Nel caso dei documenti informatici, il sistema prevede anche la registrazione dell'impronta, cioè di una sequenza di caratteri che identificano in maniera univoca l'integrità del documento stesso.

Segnatura (Timbro di protocollo)

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile. La registrazione e la segnatura costituiscono un'operazione unica e contestuale aventi entrambe la natura di atto pubblico. Nel caso di documenti relativi a gare d'appalto che vengono protocollati in busta chiusa, la segnatura verrà apposta sulla busta stessa. Nel documento cartaceo in arrivo la segnatura viene posta, di norma, sul fronte attraverso un timbro. In caso di documento informatico la segnatura viene creata con apposita funzione informatica e associata al documento informatico.

Unicità del numero di protocollo

Ogni documento, indipendentemente dalla natura (in arrivo o in partenza), deve essere individuato da un numero di protocollo univoco. Pertanto non è assolutamente consentito l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza, neppure se la pratica si esaurisce con la risposta e neppure se la registrazione avviene nel medesimo giorno lavorativo.

Solo nel caso di documenti in partenza con più destinatari è consentita la spedizione di più copie del documento identificate dallo stesso numero di protocollo. In tal caso nella registrazione di protocollo vanno riportati i nominativi di tutti i destinatari, qualora ciò non contrasti con specifiche procedure amministrative come ad es. alcune tipologie di gara.

Classificazione

La classificazione avviene identificando all'interno del Titolario di Classificazione a quale elemento gerarchico dello stesso il documento è riferibile (Indice di classificazione).

Scansione Ottica

Per i documenti in arrivo in formato cartaceo, in questa fase si procede alla loro “scansione ottica”. La “scansione ottica” viene effettuata con uno “scanner” a cura di **SPI**. Nell’Allegato 1 vengono indicate le caratteristiche dello strumento da impiegare e le caratteristiche dei documenti che per mole o formato non sono oggetto di obbligo di “scansione ottica”.

Documenti soggetti ad obbligo di protocollazione

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall’Amministrazione e tutti i documenti informatici, ne sono esclusi:

- gazzette ufficiali;
- bollettini ufficiali P. A.;
- notiziari P. A.;
- note di ricezione di circolari;
- note di ricezione di altre disposizioni;
- materiali statistici;
- atti preparatori interni;
- corrispondenza interna dell’Amministrazione con esclusione dei documenti dai quali possono nascere diritti, doveri o legittime aspettative di terzi (es. comunicazione di risoluzione del rapporto di lavoro, domanda di collocamento a riposo, richiesta di mobilità o simili, presentate dai dipendenti del Comune);
- giornali;
- riviste;
- libri;
- materiali pubblicitari;
- offerte, preventivi non richiesti formalmente con lettera protocollata;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- inviti a corsi, convegni, forum, progetti formativi e stage;
- certificato di situazioni retributive e contributive del personale;
- estratti conto;
- lettere accompagnatorie di fatture;
- comunicazione da parte di Enti di bandi di concorso e di domande da presentare;
- avvisi o comunicazioni da pubblicare all’Albo Pretorio;
- biglietti d’occasioni (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
- bolle di accompagnamento;
- giustificativi relativi a permessi vari dei dipendenti comunali, obiettori, lavoratori socialmente utili ecc.;
- certificati e simili;
- tutti i documenti già soggetti a registrazione particolare dell’Amministrazione;
- documenti di competenza di altre Amministrazioni.

Qui di seguito sono descritti i criteri di trattazione dei seguenti tipi di documento:

- **Documenti anonimi:** le lettere anonime sia in formato cartaceo che in formato elettronico vanno protocollate. In questi casi, si prevede di indicare come mittente: “mittente anonimo”. Tali documenti saranno sempre definiti con livello di riservatezza pari a 3 (riservatezza alta)

- **Documenti non firmati:** i documenti sia in formato cartaceo che in formato elettronico privi di firma o con firma illeggibile vanno di norma protocollati. E' compito di **RUOR** valutare, caso per caso ai fini della sua efficacia riguardo ad una pratica o ad un determinato procedimento amministrativo, se il documento privo di firma o con firma illeggibile debba essere ritenuto comunque valido ed accettato.
- **Documenti ricevuti a mezzo Telefax:** i documenti ricevuti a mezzo Telefax devono essere sottoposti a scansione ottica indipendentemente dal numero di pagine di cui sono composti e trattati conseguentemente come documento pervenuto in formato cartaceo in accordo al contenuto dell'Art. 27 della Sez. IV del MANUALE. Occorre qui ribadire che ogni documento deve essere individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione. Di conseguenza qualora venga successivamente ricevuto lo stesso documento in originale, **RSPI** deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax se possibile e giuridicamente corretto.
- **Documenti ricevuti sulla Casella di Posta Elettronica Istituzionale:** i messaggi di posta elettronica che soddisfano i requisiti indicati dalla normativa vigente vanno protocollati. Potranno essere protocollati sia il corpo del messaggio che uno o più dei file ad esso allegati, purché corredati di firma digitale, secondo le indicazioni della normativa vigente. L'eventuale segnatura di protocollo dovrà rispettare lo standard XML.

Annullamento o modifica di una registrazione

Nel seguito vengono fornite le regole per l'annullamento o la modifica di una registrazione di protocollo. (Art. 54 DPR 445/2000):

- È consentito l'annullamento di una registrazione di protocollo solo tramite l'apposizione della dicitura «annullato» o simbolo di significato analogo, che deve essere effettuata in maniera tale da consentire la lettura delle informazioni registrate in precedenza e da non alterare le informazioni registrate negli elementi obbligatori del protocollo. **RSPI** è l'unico autorizzato ad annullare una registrazione di protocollo. Le richieste di annullamento per la relativa autorizzazione vanno inoltrate a **RSPI** tramite la Casella Interna di **SPI** con l'indicazione del numero di protocollo da annullare, indicando i motivi dell'annullamento. Associata alla registrazione di protocollo originale deve apparire in forma ben visibile, oltre agli elementi già indicati, la data dell'operazione, il codice identificativo dell'addetto che ha effettuato l'annullamento e gli estremi del provvedimento di autorizzazione. Deve essere previsto un registro che contiene le richieste di annullamento e le relative autorizzazioni.
- I seguenti dati di una registrazione di protocollo vanno considerati imm modificabili:
 - numero di protocollo del documento generato automaticamente dal sistema;
 - data di registrazione di protocollo assegnata automaticamente dal sistema;
 - mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
 - oggetto del documento;

- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica.

Eventuali modifiche ai sopraelencati dati vanno trattate a tutti gli effetti come le operazioni di annullamento di registrazioni disciplinate al punto precedente.

Registro giornaliero di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici a favore o a danno delle parti. Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Al fine di tutelare l'integrità e la regolarità delle registrazioni, **RSPI** deve provvedere quotidianamente alla stampa del registro giornaliero di protocollo. Entro il mese di gennaio, **RSPI** provvede alla stampa del registro di protocollo dell'anno precedente e, verificata la congruità delle registrazioni, allo scarto delle eventuali stampe del registro giornaliero di protocollo dell'anno precedente. Al fine di mantenere anche su supporto cartaceo, traccia delle eventuali modifiche degli elementi accessori del protocollo, intervenute per effetto della gestione dei documenti e dei procedimenti amministrativi, **RSPI** provvede entro il mese di gennaio alla stampa e alla rilegatura del registro di protocollo relativo al quinto anno antecedente.

Tenuto conto che: "il sistema deve consentire la 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" (art. 53, comma 2, DPR 445/2000), nel seguito vengono specificate le modalità di produzione e conservazione del registro giornaliero informatico di protocollo:

- al fine di consentire alle **UOR** le operazioni di registrazione di protocollo in ore anche successive a quella di chiusura degli Uffici di **SPI**, l'operazione di stampa del registro relativa alle registrazioni effettuate nell'arco di uno stesso giorno viene effettuata come prima operazione del mattino del primo giorno lavorativo successivo;

Tenuto altresì conto che: "Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, deve essere riversato su supporti informatici non riscrivibili e deve essere conservato da soggetto diverso dal responsabile del servizio appositamente nominato da ciascuna Amministrazione" Art. 7, comma 5 del DPCM 31 ottobre 2000, nel seguito vengono descritte le istruzioni per effettuare il salvataggio:

- il responsabile del salvataggio è **RSPI** o un suo delegato il cui nominativo è indicato nell'Allegato 2;
- **RSPI** provvederà ad individuare il nominativo dell'incaricato alla conservazione dei supporti e il suo vicario per casi di vacanza, assenza o impedimento.
- il vicario ha solo il compito di provvedere a prendere in consegna da **RSPI** i supporti in caso di assenza dell'addetto della conservazione e di consegnarli a questo ultimo nell'arco del mattino del primo giorno lavorativo di presenza dello stesso;
- è compito del vicario segnalare a **RSPI** in quali giorni subentra alle funzioni di presa in carico dei supporti solitamente svolte dall'addetto della conservazione degli stessi;
- considerazioni di opportunità legate all'esistenza di particolari attività non rimandabili (ad. es. registrazioni di documenti in occasione di elezioni, eventi

inerenti la “Protezione Civile”, ecc.) impongono all’Amministrazione di identificare la dicitura “termine della giornata lavorativa” citata dalla norma con la mezzanotte di ogni giorno lavorativo;

- il salvataggio deve essere effettuato, relativamente alle registrazioni effettuate nell’arco di uno stesso giorno, come seconda operazione del mattino del primo giorno lavorativo successivo e quindi immediatamente dopo l’operazione di stampa del registro giornaliero di protocollo. E’ assolutamente esclusa la possibilità che il salvataggio sia effettuato in tempi significativamente differiti rispetto alla stampa del registro giornaliero di protocollo relativo alla stessa giornata di attività. Il lasso di tempo intercorrente fra le due operazioni deve essere solo quello giustificato dalla distinta modalità tecnica di realizzazione delle due operazioni;
- considerata l’impossibilità da parte del sistema di effettuare registrazioni in data anteriore a quella del giorno in corso, la procedura di salvataggio può essere eseguita anche in presenza di stazioni di lavoro già operanti;
- la funzione di salvataggio deve provvedere a memorizzare su di uno specifico archivio permanente del server che ospita l’archivio del protocollo corrente, un record per ogni salvataggio eseguito prevedendo la memorizzazione di almeno i seguenti dati:
 - la numerazione progressiva del salvataggio nel corso dell’anno;
 - la data di riferimento delle operazioni di protocollazione riportate;
 - la data di esecuzione del salvataggio;
 - l’ora di esecuzione del salvataggio;
 - i primo ed ultimo numero di protocollo oggetto di memorizzazione.

I dati sopra indicati dovranno essere oggetto della stampa di una etichetta che l’operatore provvederà a posizionare sul supporto non riscrivibile e removibile usato (CD ROM) e di una ricevuta di consegna in duplice copia delle quali una è destinata al responsabile della conservazione del supporto stesso. La copia della ricevuta controfirmata dall’addetto della conservazione del supporto o dal suo vicario, dovrà essere conservata da **RSPI** nello stesso luogo di conservazione dei registri giornalieri di protocollo;

- è compito di **RSPI** verificare e garantire che i dati contenuti sulla etichetta e sulla ricevuta di consegna siano identici a quelli prodotti dalla stampa del registro giornaliero di protocollo di pari numero progressivo. La presenza della firma di **RSPI** sull’etichetta e sulla ricevuta garantiscono il buon esito della verifica di cui sopra;
- prima che sia eseguita la fase di salvataggio, la procedura dovrà verificare il valore dell’ultimo numero di protocollo salvato nella precedente sessione rispetto a quello del primo che sarà oggetto di salvataggio. In caso non esista continuità fra i due numeri la procedura dovrà provvedere a segnalarlo e nel contempo disabilitare in modo permanente l’utilizzo delle funzioni di protocollazione, finchè non verrà trovata la causa di errore e ripristinata la corretta situazione dell’archivio;
- prima che sia eseguita la fase di salvataggio, la procedura dovrà permettere la verifica che il supporto non riscrivibile che verrà utilizzato non contenga alcuna registrazione, in caso contrario darà una segnalazione all’operatore e terminerà;
- il buon esito della funzione di salvataggio dovrà essere comunicato all’operatore solo dopo che la stessa avrà effettuato la memorizzazione del “record di salvataggio” sull’archivio permanente sul server e verificata la presenza sul supporto non riscrivibile delle registrazioni che erano oggetto di salvataggio;
- la procedura di salvataggio dovrà essere dotata di funzionalità di ripartenza automatica in grado di ripristinare a seguito di una qualsiasi causa di interruzione la

situazione pregressa degli archivi informatici allo stato in cui erano all'atto del comando di esecuzione della stessa;

- **RSPI** provvederà a consegnare all'addetto della conservazione, il supporto munito di etichetta firmata relativo ad una giornata di attività nell'arco del mattino del successivo giorno lavorativo unitamente ad una copia della ricevuta di consegna. All'atto della consegna del supporto l'etichetta presente sul supporto andrà controfirmata dall'addetto della conservazione o suo vicario.

Registro di emergenza

Premettiamo che in caso di interruzione per qualsiasi causa delle funzionalità del Sistema di Gestione Informatica dei Documenti, situazione definita di emergenza, le fasi di trattamento dei documenti che debbono essere garantite sono solo le seguenti:

- produzione (solo documenti la cui spedizione non è rimandabile in alcun modo);
- ricezione;
- classificazione e protocollazione;
- spedizione.

L'unica fase di competenza delle **UOR** sarà quella di produzione, mentre tutte le altre saranno effettuate centralmente presso **SPI**. Nelle situazioni di emergenza ogni evento deve essere registrato su un supporto cartaceo, denominato Registro di Emergenza. Per la tenuta del registro di emergenza è possibile utilizzare strumenti informatici dedicati che non necessitano di connessione in rete con il Sistema Centrale. Ovviamente solo il registro cartaceo, anche in forma stampabile da apposito software applicativo, ha valore. I dati registrati su supporto magnetico possono avere solo la funzione, una volta che siano opportunamente verificati tramite il confronto con i contenuti del registro cartaceo, di essere di ausilio nella fase di recupero delle registrazioni al ripristino della funzionalità del sistema informatico.

Sul registro di emergenza debbono essere indicate:

- la causa dell'interruzione;
- la data di interruzione;
- l'ora di inizio dell'interruzione;
- la data e l'ora del ripristino della piena funzionalità del sistema informatico;
- eventuali annotazioni ritenute rilevanti da **RSPI**.

Viene costituito un unico registro di emergenza presso **SPI**. **RSPI** dovrà annotare nel protocollo unico i periodi di attivazione del registro di emergenza. Qualora nel corso di un anno non si sia fatto ricorso al registro di emergenza, se ne deve annotare anche il mancato uso.

Nel registro di emergenza ogni documento è individuato da:

- numero assegnato nel registro di emergenza;
- **UOR** competente;
- anno di registrazione;
- numero di protocollo.

Una volta ripristinata la piena funzionalità del sistema, **RSPI** provvede alla chiusura della sessione di emergenza, annotando sul registro il numero delle registrazioni effettuate e la

data e l'ora di chiusura e provvede senza ritardo all'inserimento delle registrazioni del Registro di Emergenza sul protocollo unico.

Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico: ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio.

A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo unico. L'efficacia della registrazione è dunque garantita dal numero attribuito nel registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo; l'efficienza, invece, verrà garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica.

A scopo di completezza formale, qui di seguito richiamiamo le specifiche per la tenuta del registro di emergenza previste dall'Art. 63 del DPR 445/2000 che hanno ispirato le istruzioni operative sopra esposte:

- **RSPI** autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino delle funzionalità del sistema;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, **RSPI** può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
- per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario della **AOO**;
- le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando una apposita funzione di recupero dei dati, senza ritardo al ripristino della funzionalità del sistema;
- durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione col numero utilizzato in emergenza;
- sul registro di emergenza viene riportato ad ogni fine giornata il numero totale di operazioni registrate manualmente.

Articolo 28: Fascicolazione

La fascicolazione dei documenti è una attività di competenza esclusiva delle **UOR** sia per documenti in arrivo che in partenza.

Occorre sottolineare che in un sistema di gestione e tenuta dei documenti ciò che più conta non è il documento in quanto tale, ma l'insieme delle relazioni che il documento ha con l'intero archivio. Più in particolare, le relazioni con gli altri documenti attinenti ad una

medesima pratica o procedimento amministrativo. La manutenzione e conservazione dei fascicoli e dei documenti ivi contenuti sono responsabilità del **RUOR** di riferimento.

La fascicolazione avviene col seguente flusso:

Documenti in arrivo

- verificata in precedenza la corretta assegnazione del documento alla **UOR**, preso in carico lo stesso ed assegnato internamente al corretto destinatario (**RPA**), questi aggiorna il livello di riservatezza del documento ed eventualmente del fascicolo. Il valore del livello di riservatezza del documento può essere aggiornato solo rendendolo più restrittivo (passaggio da valore medio ad alto oppure passaggio da valore basso a medio). Il valore di riservatezza precedente deve comunque essere memorizzato separatamente per memoria. **RPA** può quindi procedere in due modi:
 - se esiste la pratica attinente al documento, seleziona il fascicolo e inserisce il documento nel fascicolo selezionato;
 - se la pratica non esiste, provvede alla sua creazione e ad aggiornare il repertorio dei fascicoli e successivamente inserisce il documento nel fascicolo. All'atto della creazione del fascicolo, **RPA** definisce il livello di riservatezza dello stesso analogamente a quanto già previsto per documenti. Inoltre in conseguenza della definizione del livello di riservatezza, **RPA** può definire specifici criteri di accesso al fascicolo in termini di funzionalità applicative di visibilità, ricerca e stampa. Una volta inserito il documento, il fascicolo viene assegnato all'istruttore.

In caso di documenti relativi a gare d'appalto pervenuti alla **UOR** in busta chiusa, prima di effettuarne la fascicolazione al termine dei lavori di espletamento delle procedure di gara, è compito di **RUOR** riconsegnarli a **SPI** al fine di consentirne la scansione ottica. Presi in carico i documenti, **SPI** verificherà la corretta compilazione della segnatura da parte di **RUOR**, provvederà ad effettuarne la scansione ottica e a ridistribuirli come documenti informatici a **RUOR** per consentire la fase di fascicolazione.

Documenti in partenza

- effettuate le fasi previste dall'Art. 25 della Sez. IV, **RPA** opera nel seguente modo:
 - se esiste la pratica attinente al documento, seleziona il fascicolo e inserisce il documento nel fascicolo selezionato;
 - se la pratica non esiste, provvede alla sua creazione e ad aggiornare il repertorio dei fascicoli, successivamente inserisce il documento nel fascicolo.

Il fascicolo è individuato da tre elementi indispensabili:

- anno di istruzione;
- numero di repertorio, progressivo annuale nell'ambito dell'ultimo livello gerarchico dell'indice di classificazione;
- oggetto, cioè un breve testo che descrive compiutamente una pratica: affare o procedimento amministrativo.

Repertorio dei fascicoli

Il repertorio dei fascicoli è un registro comprendente almeno i seguenti elementi:

- anno di istruzione;
- indice di classificazione;
- numero del fascicolo;
- oggetto del fascicolo;
- data di chiusura corrispondente alla data dell'ultimo documento fascicolato;
- annotazione del passaggio dall'archivio corrente all'archivio di deposito;
- annotazione del passaggio dall'archivio di deposito a quello storico o, in alternativa, l'avvenuto scarto.

I documenti sono archiviati all'interno di ciascun fascicolo rispettandone l'ordine cronologico di registrazione. In base, cioè, al numero di protocollo ad essi attribuito o, se assente, in base alla propria data.

Oltre ai fascicoli relativi ad affari o procedimenti amministrativi esistono fascicoli nominativi per ogni unità di personale dell'Amministrazione. Il fascicolo viene aperto al momento dell'assunzione o riaperto nel caso di ripristino del rapporto di lavoro. Il fascicolo viene chiuso al momento in cui cessa il rapporto di lavoro. I fascicoli del personale costituiscono una serie archivistica, da conservare in ordine di matricola o, se assente, in ordine alfabetico per cognome e nome.

Articolo 29: Spedizione

La spedizione dei documenti è una attività di competenza sia di **SPI** che delle **UOR**.

La fase di spedizione avviene con le seguenti modalità:

- a carico di **SPI** nel caso di documenti in formato cartaceo successivamente all'operazione di affrancatura. La spedizione deve avvenire di norma nello stesso giorno lavorativo di protocollazione da parte della **UOR**;
- a carico della **UOR** nel caso di documenti cartacei oggetto di trasmissione via telefax;
- a carico della **UOR** nel caso di documenti in formato elettronico, con l'invio dalla Casella di Posta Elettronica Istituzionale dell'Amministrazione alla casella di posta del destinatario.

Sarà cura di **SPI** e delle **UOR** verificare, preliminarmente alla spedizione di qualsiasi documento in formato cartaceo, se il destinatario è in grado di riceverlo come documento informatico spedito per via telematica. E' opportuno in tal senso che **SPI** e le **UOR** collaborino per realizzare quanto prima un indirizzario elettronico degli interlocutori esterni.

Articolo 30: Archiviazione e conservazione

Il processo di archiviazione e conservazione dell'archivio di deposito è una attività condivisa da **SPI** e dalle **UOR**.

L'archiviazione e conservazione dell'archivio di deposito si articola nelle fasi di:

Selezione

- **UOR** seleziona le pratiche da considerarsi chiuse o comunque non più necessarie ad una trattazione corrente e le rende disponibili a **SPI** corredandole di apposito verbale di consegna. L'operazione di definizione della chiusura delle pratiche da parte delle **UOR** può essere distribuita nel corso della gestione, mentre la selezione avviene di norma una volta all'anno entro una data definita in accordo a **RSPI** e comunque riguarderà le pratiche definite chiuse nel corso dell'anno precedente;
 - l'avvenuta operazione di selezione va segnalata da ogni **UOR** tramite opportuno messaggio indirizzato alla Casella Interna di **RSPI** con allegato il verbale di consegna.

Versamento

- **RSPI** predispone un elenco di consistenza, riscontra i singoli verbali di consegna comunicando agli **RUOR** l'operazione effettuata (verbale di versamento), prende in carico i fascicoli e li memorizza nell'archivio di deposito.
 - Dopo ogni aggiornamento dell'archivio di deposito, **RSPI** provvederà ad effettuarne almeno due copie di salvataggio che custodirà in idonei locali.

I dettagli operativi per gestire in sicurezza l'operazione di selezione e versamento sono elencati nell'Art. 50 della Sez. VI.

Le serie archivistiche

Presso l'Amministrazione sono attivi i repertori indicati nell'Allegato 5.

Le serie archivistiche relative agli ultimi cinque anni sono conservate presso l'Ufficio Segreteria; trascorso tale termine, le serie e i repertori vengono conferiti a **RSPI** che provvede ad archivarle.

L'archivio storico

La formazione, conservazione e consultazione dell'archivio storico sono attività di competenza di **SPI** e prevedono le seguenti fasi:

- analisi dei documenti da archiviare;
- selezione dei documenti a cui applicare lo scarto di archivio;
- versamento dei documenti nell'archivio storico;
- riordino e inventariazione;
- conservazione del patrimonio documentario;
- gestione degli accessi a terzi per consultazione.

Le modalità di realizzazione delle attività elencate sono descritte agli Art. 22 e 23 della Sez. III del MANUALE e nell'Allegato 4 e 5.

SEZIONE V: Flussi di Lavorazione dei Documenti

Articolo 31: Distribuzione con assegnazione dei documenti in arrivo

Il processo di distribuzione con assegnazione dei documenti in arrivo è una attività condivisa da **SPI** e dalle **UOR**.

La distribuzione con assegnazione avviene col seguente flusso:

- **SPI** individua la **UOR** di competenza per la fase di fascicolazione verificando se il documento prevede un destinatario nominalmente predefinito:
 - in caso affermativo e si hanno ragioni di ritenere che per la natura del documento il destinatario sia corretto ed abilitato al livello di riservatezza del documento, procede all'inoltro del documento al destinatario;
 - in caso non sia predefinito il destinatario oppure non esistano ragioni per ritenere che per la natura del documento il destinatario sia corretto, procede all'inoltro del documento a **RUOR**;
- inoltro del documento, munito dei riferimenti di protocollo e della indicazione del destinatario, dalla Casella Interna di **SPI** alla Casella Interna di **RUOR**. La spedizione avviene con ricevuta di ritorno utilizzata da **SPI** per cancellare il documento dalla posta in ingresso:
 - se **RUOR** valuta non corretta l'assegnazione, rispedisce il documento a **SPI** munito delle eventuali osservazioni di merito; ad esempio le eventuali informazioni in suo possesso per coadiuvare **SPI** nel successivo tentativo di assegnazione. La spedizione avviene con ricevuta di ritorno utilizzata da **RUOR** per cancellare il documento dalla propria Casella Interna. Rimane assolutamente esclusa la possibilità che il documento venga inoltrato direttamente ad altra **UOR**. Anche in caso di errata assegnazione, il **RUOR** destinatario è comunque vincolato al trattamento del documento nel rispetto del livello di riservatezza attribuito da **SPI**;
 - se **RUOR** valuta corretta l'assegnazione:
 - provvede alla presa in carico del documento. In caso di documenti relativi a gare d'appalto assegnati e distribuiti in busta chiusa, è compito di **RUOR** all'atto dell'apertura della busta riportare sui documenti contenuti i dati di segnature già presenti sulla busta;
 - attiva l'assegnazione interna anche in deroga all'indicazione del destinatario originale purchè in accordo ai requisiti di compatibilità con il livello di riservatezza attribuito. Per effettuare l'assegnazione interna, **RUOR** individua il nominativo di **RPA** se preesistente, oppure trattiene il documento che considera assegnato a se stesso oppure può, ai sensi dell'art 5 della legge 241/90, assegnare ad altri la responsabilità del procedimento o della pratica, individuando in quel momento il **RPA** all'interno della propria **UOR**.

Articolo 32: Gestione integrata dei fascicoli, dei flussi documentali e dei procedimenti amministrativi

Le entità coinvolte in questa fase sono solo le **UOR**, che hanno responsabilità sull'avvio e sul monitoraggio dei flussi documentali. Fermi restando i limiti di ambito di applicazione del manuale descritti nell'Art. 2 della Sez. I, è compito di **RPA** gestire comunque il monitoraggio del flusso di lavorazione dei documenti.

In pratica, **RPA** ha l'onere di registrare manualmente i flussi di lavorazione e di aggiornare lo stato di avanzamento della pratica.

L'eventuale passaggio di documenti o fascicoli tra le varie **UOR** avviene con il seguente schema:

- la **UOR** mittente seleziona i documenti/fascicoli da trasmettere e li spedisce alla Casella Interna della **UOR** destinataria con ricevuta di ritorno che serve alla **UOR** mittente per procedere alla eliminazione dei documenti/fascicoli inviati;
- la **UOR** destinataria prende in carico la documentazione spedita, le assegna un **RPA** (che eventualmente assegna nuovamente il livello di riservatezza dei fascicoli e dei documenti) ed avvia il nuovo procedimento.

Questo schema si basa su una gestione manuale del flusso documentale e prelude ad una futura estensione dell'ambito del MANUALE. L'invio e la ricezione delle ricevute di ritorno, così come la cancellazione della documentazione inviata da parte della **UOR** mittente, non saranno più necessarie qualora si adottino strumenti informatici di supporto alla gestione delle attività (workflow).

SEZIONE VI: Accessibilità e Sicurezza dei Documenti

Articolo 33: Caratteristiche del Piano della Sicurezza dei Documenti Informatici

In riferimento ai processi e ai flussi definiti nelle Sez. IV e V, in questa Sezione verranno descritte le Analisi dei Rischi, le Politiche di Sicurezza e gli Interventi Operativi al fine di ottemperare a quanto prescritto dall'art. 4 comma 1 lett. c del DCPM 31/10/2000 .

Tra gli obiettivi e i compiti di **RSPI** si prevede in particolare la predisposizione del piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con **RSIA** e con **RSDP** di cui alla legge 31 dicembre 1996, n° 675 ora D.Lgs. 196/03, e successive modificazioni e integrazioni, e nel rispetto delle misure minime di sicurezza previste la regolamento di attuazione emanato con DPR 28 luglio 1999, n° 318, in attuazione dell'art. 15 comma 2 della citata legge 675/1996”.

Il presente Piano della Sicurezza dei Documenti Informatici è conforme al dettato dell'art. 10 della deliberazione AIPA 51/2000:

- le pubbliche amministrazioni predispongono, entro dodici mesi dalla data di entrata in vigore della presente deliberazione, un piano per la sicurezza informatica relativo alla formazione e alla conservazione dei documenti informatici;
- il piano fa parte del manuale di gestione di cui alle regole emanate ai sensi del DPR 20 ottobre 1998, n° 428;
- il piano considera almeno i seguenti aspetti: analisi dei rischi, politiche di sicurezza, interventi operativi;
- il piano è sottoposto a verifica ed aggiornato con cadenza almeno biennale;
- le pubbliche amministrazioni adottano le misure minime di sicurezza dei dati personali ai sensi dell'art. 15 della legge 31 dicembre 1996, n° 675 ora D.Lgs. 196/03, e del relativo regolamento di attuazione emanato con DPR 28 luglio 1999, n° 318.

Gli argomenti trattati in questa sezione del MANUALE non riguarderanno gli ambiti più generali della sicurezza delle informazioni, già disciplinati da altri documenti dell'Amministrazione soprattutto per ciò che concerne l'infrastruttura tecnologica che è condivisa con il restante Sistema Informatico. I contenuti della sezione riguarderanno esclusivamente gli aspetti specifici della sicurezza dei documenti informatici. Ciò in considerazione che tali formati di documenti non hanno ancora trovato una loro collocazione nel Sistema di Gestione della Sicurezza delle Informazioni in quanto sino al momento istitutivo di **SPI** la loro eventuale presenza informale, sostanzialmente in qualità di duplicato di documenti cartacei da considerarsi originali, non poteva che essere ignorata.

Articolo 34: Analisi dei rischi

L'Analisi dei Rischi a cui sono esposti i documenti informatici, redatta per ambiti di lavorazione, funzioni di gestione e tipologia di documento, è riportata nell'Allegato 6.

Politiche di Sicurezza ed Interventi Operativi: Misure di Carattere Generale

Articolo 35: Accesso fisico agli uffici di SPI, SIA e delle UOR

Nel seguito vengono elencate le misure di salvaguardia dell'accesso fisico ai locali destinati all'esercizio delle attività di **SPI**, **SIA** e **UOR** inerenti all'oggetto del MANUALE:

- Tutto il personale di **SPI**, **SIA** e il personale delle **UOR** addetto alle fasi di gestione della documentazione è edotto sulla necessità di controllare l'accesso fisico agli uffici, e sui rischi che derivano dalla presenza di persone non autorizzate. Nel caso di uffici aperti al pubblico, l'Amministrazione provvederà a delimitare specifiche aree di accesso controllate.
- I documenti con livello di riservatezza medio o alto (vedi Art. 36 della Sez. VI), i documenti la cui riservatezza non è stata ancora classificata e tutte le componenti degli impianti di elaborazione dati devono essere adeguatamente protetti da modifiche, furti, e divulgazione non autorizzata.
- Sono considerati "aree di sicurezza" i locali che contengono particolari apparecchiature di elaborazione o comunicazione dati (server, hub, router, stazioni di lavoro abilitate a funzionalità inerenti l'oggetto del MANUALE, ecc.) che devono essere protette in modo specifico. In particolare i locali destinati a garantire la continuità del servizio in caso di emergenza (vedi Art. 43 della Sez. VI) ed i locali destinati alla conservazione delle copie di salvataggio di qualsiasi tipo, devono essere considerati "aree di sicurezza".
- L'accesso alle aree di sicurezza è vietato:
 - alle persone estranee a **SPI** che non siano autorizzate da **RSPI** per ciò che riguarda le aree che ospitano le stazioni di lavoro abilitate a funzionalità applicative inerenti l'oggetto del MANUALE;
 - alle persone estranee a **SIA** che non siano autorizzate da **RSIA** per ciò che riguarda tutte le apparecchiature;
 - alle persone estranee alla **UOR** che non siano autorizzate da **RUOR** per ciò che riguarda l'accesso ai locali che ospitano le stazioni di lavoro abilitate a funzionalità applicative inerenti l'oggetto del MANUALE.

Non è consentita la presenza nelle aree di sicurezza di persone che non siano accompagnate (inclusi tecnici di manutenzione e personale di terze parti) e non sono consentite autorizzazioni verbali né dirette né telefoniche.

- Le aree di sicurezza non presidiate dagli addetti devono essere chiuse a chiave e la chiave deve essere custodita in modo sicuro da una persona responsabile. Non è consentito lasciare aperto l'ingresso di un'area di sicurezza non presidiata da personale autorizzato. Nel caso si lascino incustoditi gli uffici per il termine dell'orario di lavoro, per la pausa pranzo o per motivi diversi, deve essere verificata l'effettiva chiusura dell'ingresso all'area di sicurezza.

Articolo 36: Livelli di riservatezza

Al personale addetto appartenente a **SPI** non si applica alcun tipo di limitazione in merito al trattamento di documenti e fascicoli riservati, mentre per gli addetti delle **UOR** valgono i criteri sotto elencati.

Vengono definiti i seguenti livelli di riservatezza per i documenti in arrivo e in partenza:

- riservatezza bassa (livello 1): documenti accessibili a tutto il personale addetto della **UOR**;
- riservatezza media (livello 2): documenti accessibili solo ad una parte del personale della **UOR**, preventivamente e formalmente autorizzato da **RUOR** con contestuale comunicazione a **SPI**;
- riservatezza alta (livello 3): documenti accessibili solo a **RUOR**. In caso di necessità, **RUOR** potrà incaricare per iscritto altri addetti di sua fiducia ad accedere ai documenti di riservatezza alta, ma ne resterà comunque responsabile.

Analogamente si opera per l'attribuzione dei livelli di riservatezza ai fascicoli. Nel seguito con la dizione "documenti riservati" o "fascicoli riservati" denoteremo i documenti o fascicoli il cui livello di riservatezza è definito come medio o alto.

Articolo 37: Profili utente e autorizzazioni d'accesso

RUOR, di concerto con **RSPI**, stabilisce i profili utente del personale della **UOR** secondo i compiti operativi attribuiti e secondo i livelli di riservatezza stabiliti.

A questo scopo (Art. 7 DPCM 31 Ottobre 2000) il software utilizzato per la gestione del servizio di protocollo informatico dovrà prevedere la possibilità di definire diversi profili di utenza e di accesso ai dati:

- profilo 1: consultazione;
- profilo 2: inserimento;
- profilo 3: modifica;
- profilo 4: annullamento.

Il significato delle diverse abilitazioni è il seguente:

- per "Consultazione" si intende la possibilità per un utente abilitato di visualizzare una registrazione di protocollo;
- per "Inserimento" si intende la possibilità per un utente abilitato di inserire i dati ed effettuare una registrazione di protocollo;
- con "Modifica" si intende la possibilità per un utente abilitato di modificare i dati di una registrazione di protocollo, con l'esclusione dei dati obbligatori;
- con "Annullamento" si intende la possibilità per un utente abilitato di annullare una registrazione di protocollo, ferme restando le regole specifiche riportate nella Sez. IV.

I profili di utenza dovranno essere inoltre distinti per funzionalità di protocollo, di fascicolazione e di accesso all'archivio di deposito.

Il personale addetto delle **UOR** ha accesso solo alle porzioni di archivio corrente contenenti le pratiche della **UOR** stessa. L'accesso ai documenti assegnati ai fascicoli è regolato dal livello di riservatezza attribuito. Analogamente l'accesso ai fascicoli è regolato dal livello di riservatezza attribuito.

Ogni addetto abilitato appartenente alle **UOR** ha associato un “account” che lo identifica in modo univoco all’interno del sistema.

L’utente accede alle funzionalità applicative digitando il suo “login” e la sua password (vedi Art. 38 della Sez. VI).

Non deve essere consentito l’accesso alle funzionalità applicative da parte di due utenti con lo stesso “account”.

Il rilascio degli account è compito di **RSPI**.

Nel caso sia necessario cancellare un account, per trasferimento dell’utente proprietario o per conclusione del rapporto di lavoro dello stesso, il responsabile della **UOR** di appartenenza è responsabile di chiederne sollecitamente la cancellazione tramite messaggio indirizzato alla Casella Interna di **RSPI**.

Analogamente si procede, sentito il parere del **RPA**, per quanto riguarda i profili utente e le autorizzazioni di accesso a singoli fascicoli in base a quanto descritto all’Art. 28 della Sez. IV.

Articolo 38: Password

Le “password” di accesso alle funzionalità applicative vengono rilasciate in versione temporanea da **RSPI**. Il personale addetto deve essere formato sul corretto uso delle password. Le password devono essere cambiate almeno ogni sei mesi. Una password corretta deve essere composta da almeno 8 caratteri, può contenere caratteri alfanumerici e non deve essere una parola di senso compiuto, o comunque una parola riconducibile all’utente o alla sua storia personale.

Per la gestione delle password valgono le seguenti regole:

- gli utenti hanno la responsabilità di scegliere e utilizzare le proprie password secondo quanto descritto nella seguente procedura;
- i singoli utenti hanno la responsabilità di gestire le loro password, modificando la password temporanea assegnatagli, con una definitiva di loro scelta;
- all’utente viene assegnata da **RSPI** una password temporanea che l’utente dovrà cambiare all’atto del primo accesso all’applicazione. L’utente dovrà indicare la password secondo quanto indicato nei punti successivi.
- la password per essere definita di qualità deve avere una lunghezza minima di otto caratteri, e deve possibilmente essere facile da ricordare, in modo da evitare eventuali trascrizioni;
- in casi specifici, quando è necessario utilizzare password che l’applicativo non è in grado di gestire con una lunghezza minima di otto caratteri, è ammesso l’utilizzo di password di lunghezza minore;
- le password non devono presentare una sequenza di caratteri identici, e non devono essere formate da gruppi di caratteri tutti numerici o tutti alfabetici;
- è molto importante che la scelta degli utenti non ricada mai su parole, deducibili da informazioni personali o dei propri familiari (come nome e cognome, numeri telefonici, date di nascita, codice fiscale, ecc...).

Per assicurare un uso corretto e sicuro, gli utenti devono attenersi ad alcune norme di comportamento:

- All'atto della prima connessione all'applicazione, l'utente dovrà modificare la password temporanea con quella scelta autonomamente. La password utilizzata deve essere ricordata. Diversamente, l'utente non potrebbe collegarsi una seconda volta; in questo caso è necessario fare una nuova richiesta, secondo i passi al punto successivo.
- Una volta in possesso della sua password, l'utente non dovrà mai trascriverla su carta, a meno che non sia possibile custodirla in modo sicuro (i criteri di sicurezza da usare sono gli stessi con cui si custodirebbe una carta di credito o un bancomat, ecc...), altresì non dovrà mai memorizzarla in un processo automatico di log-on, ad esempio in una macro o in un tasto funzionale.
- Nel caso all'utente si presentasse una qualsiasi indicazione di possibile invalidazione del sistema o della password, deve immediatamente modificare la sua password e notificare l'accaduto al personale responsabile della gestione degli incidenti appartenente a **SPI**.
- Tutte le password devono essere sostituite ogni sei mesi, a partire dalla loro creazione.
- Le password non devono essere riciclate. A tale scopo il sistema prevede una procedura di controllo sulla creazione delle password.
- E' essenziale che gli utenti mantengano le password confidenziali (non condividere singole password utente), questo non solo per motivi di sicurezza, ma anche per tutelare se stessi.

In caso sia necessario richiedere una nuova password temporanea (per incidenti, malfunzionamenti, ecc.) occorre inoltrare richiesta scritta (anche tramite messaggio indirizzato alla Casella Interna) a **RSPI**, che provvede a fornire la nuova password temporanea direttamente all'utente in busta chiusa.

Articolo 39: Clear screen e clear desk policy

A prescindere dal livello di riservatezza dei documenti trattati e dal profilo utente, tutto il personale addetto deve osservare una serie di regole di comportamento:

- I documenti, soprattutto quelli con livello di riservatezza media ed alta, nel seguito più brevemente definiti come documenti riservati, non devono essere lasciati incustoditi sulle scrivanie. I documenti riservati devono essere conservati sotto chiave quando non sono utilizzati e soprattutto fuori dall'orario di lavoro.
- È buona norma al termine dell'orario di lavoro lasciare la scrivania sgombra da documenti di qualsiasi tipo.
- Le stazioni di lavoro devono essere bloccate quando non sono sorvegliate ed utilizzate. In caso di assenza dell'addetto per un periodo superiore ai trenta minuti è obbligatorio spegnere la stazione di lavoro. Per periodi inferiori è obbligatorio bloccare l'accesso alla stazione di lavoro con le apposite funzioni del sistema operativo. È buona norma in tutti i casi in cui ci si allontana dal posto di lavoro sconnettersi dagli applicativi in uso.

Articolo 40: Le stampe

L'impiego di strumenti informatici o di fotocopie in grado di produrre documenti cartacei amovibili necessita di definire specifiche regole di comportamento per gli addetti:

- Il personale addetto è responsabile dei documenti che stampa o riproduce. Nel caso di stampanti di rete, l'utente deve ritirare la stampa con sollecitudine, non lasciando la stampante incustodita per evitare che i documenti stampati possano essere sottratti, anche temporaneamente, da persone non autorizzate .
- In ogni caso la produzione di stampe, specialmente se di documenti riservati o contenenti informazioni riservate, deve essere ridotta al minimo indispensabile, e il documento stampato va trattato con le stesse politiche osservate per l'originale.
- Se è necessario fare un fax di un documento riservato, non deve essere utilizzata la funzione di memorizzazione del documento presente in alcuni modelli di fax. Utilizzare l'invio diretto del documento.
- Nei locali ove vengono trattate informazioni o documenti riservati le fotocopiatrici devono essere presidiate, in modo da evitarne l'uso non autorizzato.

Articolo 41: Protezione da software malizioso e da intrusioni esterne

RSIA ha la responsabilità della scelta dei software antivirus, di verificarne con cadenza periodica l'efficacia e di aggiornare i file di dati dei software antivirus.

Gli utenti hanno la responsabilità di segnalare tempestivamente la presenza di attività sospette sui propri sistemi al personale responsabile di gestire la rete.

Tutti le stazioni di lavoro che comunicano con l'esterno (via internet, con collegamenti dedicati, attraverso floppy disk o altri supporti removibili) devono essere adeguatamente protetti contro le minacce da software malizioso e da attacchi esterni.

Per assicurare una efficace protezione da software malizioso e da intrusioni esterne occorre attenersi alle seguenti norme di comportamento:

- Gli addetti abilitati alla comunicazione con l'esterno (invio/ricezione) debbono ricevere una formazione sui rischi legati al software malizioso e sul corretto utilizzo della posta elettronica (con particolare riferimento allo "spamming") e degli strumenti di scansione.
- Prima di caricare un qualunque tipo di dato o programma da un supporto esterno (floppy disk, CD, ecc..) gli addetti devono procedere alla scansione del supporto utilizzando l'antivirus messo a disposizione dal **SIA**.
- Gli addetti si impegnano a non modificare per nessun motivo la configurazione hardware e software della loro stazione di lavoro e a non interrompere le funzioni automatiche del software antivirus. In caso contrario, le eventuali conseguenze dovute alla presenza di virus saranno di responsabilità della **UOR**.
- Il software antivirus deve essere installato su tutti i sistemi (stazioni di lavoro e server) connessi alla rete informatica dell'Amministrazione e configurato in modo tale da essere residente in memoria e costantemente aggiornato.
- All'atto della ricezione di ogni messaggio di posta elettronica e file provenienti dall'esterno devono essere sottoposti a scansione.
- La verifica del software malizioso e la protezione da attacchi esterni deve essere eseguita a livello di "firewall" e/o sul server di Posta Elettronica; questo permette una scansione centralizzata di tutti i messaggi provenienti da Internet.

Articolo 42: Salvataggio dei dati correnti

RSIA ha la responsabilità di individuare gli strumenti e i metodi per garantire il salvataggio (backup) di qualità degli archivi correnti e delle basi dati documentali.

RSPI e **RUOR** hanno la responsabilità della gestione dei backup rispettivamente per ciò che concerne gli archivi centralizzati ed i documenti in fase di elaborazione presenti sulle stazioni di lavoro.

Per le operazioni di backup degli archivi documentali centralizzati vanno utilizzati tre set di cassette magnetiche, che devono essere utilizzate a rotazione, in modo da mantenere tre generazioni di backup.

Il backup deve essere eseguito come ultima operazione serale, e il controllo che l'operazione sia andata a buon fine deve essere effettuato come prima operazione mattutina da parte di **RSIA**. Il controllo che l'operazione di backup è andata a buon fine deve comportare l'identificazione del contenuto degli archivi presenti sulle cassette magnetiche e non limitarsi alle denominazioni degli archivi, alle date di creazione o alle loro dimensioni. Del criterio assunto da **RSIA** per effettuare il controllo su di ogni singolo archivio deve essere tenuta traccia in apposito registro.

Criteri di gestione delle cassette magnetiche destinate a contenere i salvataggi dei dati:

- le cassette devono essere sostituite ogni quattro mesi;
- le cassette da smaltire devono essere cancellate in modo sicuro;
- le cassette nuove devono riportare la data di inizio utilizzazione, in modo che possa essere controllato il periodo di effettivo uso.

Le operazioni di backup dei documenti in fase di elaborazione presenti sulle stazioni di lavoro vanno condotte effettuando copie di salvataggio negli appositi spazi predisposti a questo scopo da **RSIA** sui server centrali. Tali operazioni vanno effettuate prima del termine dell'orario di lavoro e sono responsabilità di **RUOR**.

Casella di Posta Elettronica Istituzionale

Occorre provvedere affinché i messaggi e relativi allegati in arrivo sulla Casella di Posta Elettronica Istituzionale siano duplicati su un elaboratore diverso (server o stazione di lavoro) da quello normalmente in uso a questo scopo presso **SPI** al fine di proteggere da perdite accidentali i documenti in ingresso non ancora protocollati:

- Tale misura minima può essere rafforzata prevedendo una duplicazione fisica della stazione di lavoro di **SPI** (stazione di lavoro di backup), da utilizzare in caso di mal funzionamento della stazione di lavoro principale.

Archivio corrente

- **SPI** al termine della giornata lavorativa dovrà provvedere al backup di tutti gli archivi documentali di interesse corrente e alla conservazione delle copie in luogo sicuro in armadi ignifughi chiusi a chiave.
- Al termine della giornata lavorativa il contenuto del registro di protocollo deve essere riversato su supporti non riscrivibili e conservato a cura del Responsabile nominato dall'Amministrazione in luogo sicuro al di fuori dei locali nella disponibilità di **SPI**. (ai sensi dell'art. 7 comma 5 del DPCM 31 ottobre 2000). Vedi Art. 27 della Sez. IV.

Per quanto attiene al salvataggio dell'archivio di deposito e di quello storico ci si deve riferire all'Art. 50 della Sez. VI.

Articolo 43: Misure per la continuità del servizio

Le misure tecniche adottate nella progettazione dell'infrastruttura tecnologica ed applicativa volte a garantire la continuità del servizio del sistema di gestione informatica dei documenti sono indicate nell'Allegato 1.

Nel seguito elencheremo pertanto le misure organizzative a carico di **SPI** e delle **UOR** che costituiscono il completamento indispensabile delle misure tecniche.

Misure a carico di SPI

RSPI ha la responsabilità di valutare tutti i rischi a cui sono esposti locali, apparecchiature, dati e personale addetto, al fine di predisporre un piano di intervento che garantisca la continuità del servizio anche in caso di interruzione della funzionalità del sistema informatico, inagibilità dei locali di SPI e carenze nella presenza del personale addetto.

Il piano di intervento formulato da **RSPI** deve assicurare la disponibilità di locali di emergenza da attivare in caso di inagibilità di quelli destinati usualmente alle attività lavorative di competenza di **SPI**. In tali locali, solitamente utilizzati dall'Amministrazione per attività non strategiche che possono agevolmente essere disponibili in tempi rapidi, devono essere predisposti strumenti di elaborazione collegati con il server centrale in grado di essere abilitati autonomamente dagli addetti di **SPI** per proseguire le attività urgenti in caso di inagibilità dei locali usualmente occupati. L'eventuale supporto informatico alla gestione del registro di emergenza deve trovare una opportuna collocazione su di un Personal Computer ivi custodito. Ugualmente negli stessi locali devono essere predisposte stazioni di lavoro specializzate in grado di interrogare supporti di backup dei dati dell'archivio corrente da impiegare per esaminare per motivi di urgenza documenti correnti od il registro di protocollo non accessibili tramite il sistema di gestione informatico dei documenti a causa dell'interruzione del servizio centrale. Ugualmente è necessario che **RSPI** individui personale delle **UOR** particolarmente esperto in grado di supportare le attività di competenza di **SPI** nei momenti critici dell'assenza degli addetti usualmente impiegati da **RSPI**.

L'uso dei locali e delle apparecchiature ivi contenute deve essere oggetto di registrazione su apposito registro contenente le seguenti indicazioni:

- periodo di utilizzo dei locali;
- addetti che vi hanno operato;
- attività svolte;
- strumentazione impiegata;
- fasi di abilitazione e disabilitazione delle apparecchiature tramite password che è stato necessario eseguire.

Per nessuna ragione al termine delle attività di emergenza ivi svolte dovranno rimanere abilitate le singole apparecchiature utilizzate.

Misure a carico delle UOR

La continuità dell'infrastruttura tecnologica utilizzata dagli addetti delle **UOR** dovrà essere garantita dal **SIA**.

RUOR deve garantire la continuità di servizio in termini di risorse umane dedicate. Ogni addetto con competenze specifiche alle attività oggetto del MANUALE dovrà avere uno o più sostituti in grado di intervenire in caso di sua assenza. La gestione del personale effettuata da **RUOR** (ferie, permessi, altri incarichi, ecc.) dovrà tener conto dell'esigenza

della continuità di servizio non solo in funzione dei propri compiti, ma anche delle attività che risultassero necessarie per garantire la continuità nella gestione degli archivi e dei flussi documentali di interesse dell'intera Amministrazione. In caso di cessazione per qualunque causa dell'attività di un addetto, il sostituto deve già essere formato in termini di competenze specifiche, di utilizzo operativo della strumentazione e delle applicazioni software. Pertanto le richieste di formazione di un addetto rivolte a **SPI** debbono sempre riguardare addetti destinati a fare funzioni di sostituti e mai addetti che debbono immediatamente divenire operativi.

Articolo 44: Tracciamento delle operazioni

Ai sensi dell'art. 7 del DPCM 31 ottobre 2000, il sistema di protocollo informatico deve garantire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

La conservazione e la verifica dei log del sistema, è responsabilità di **RSIA**.
In ogni caso, una corretta tracciatura delle operazioni deve almeno prevedere:

- le registrazioni delle attività sulla risorsa, con le seguenti indicazioni:
 - l'identificativo dell'utente;
 - dati e tempi di log-on/log-off;
 - identificazione ed ubicazione della stazione di lavoro se possibile;
 - tentativi di accesso al sistema, riusciti o non;
 - tentativi di accesso a dati e risorse, riusciti e non;
- l'ordine e la frequenza con la quale saranno esaminati i dati di log;
- la persona responsabile dell'attività di visione dei dati di monitoraggio;
- l'indicazione sul tempo di conservazione delle registrazioni;
- uno storico sugli incidenti;
- la gestione degli incidenti.

Il tracciamento degli accessi all'archivio di deposito deve essere effettuato separatamente a quello dell'archivio corrente, ma con le stesse caratteristiche sopra indicate.

Copia di ogni tracciamento settimanale degli accessi all'archivio corrente ed a quello di deposito deve essere consegnata da **RSIA** a **RSPI** tenendone traccia in apposito registro.

Politiche di Sicurezza ed Interventi Operativi: Misure di Sicurezza relative alle Fasi di Lavorazione

Articolo 45: Produzione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- la produzione del documento deve avvenire secondo i dettati previsti dalla normativa per la formazione dei documenti informatici;
- dal momento in cui il documento viene firmato digitalmente da **RPA**, che assegna il livello di riservatezza, il documento deve essere memorizzato esclusivamente sul server dedicato nella partizione logica accessibile alla **UOR** di competenza. Da questo momento il documento è accessibile solo da coloro che possiedono l'abilitazione necessaria al grado di riservatezza assegnato;
- una volta firmato digitalmente, il documento diviene immodificabile: pertanto l'accesso dovrebbe essere di sola lettura;
- dal momento in cui il documento entra a far parte del sistema documentale, ogni altra copia precedente del documento deve essere cancellata (dalle stazioni di lavoro, da cartelle di transito o temporanee, ecc.).

Articolo 46: Ricezione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- Una volta assegnati i livelli di riservatezza ai documenti in arrivo, dovranno essere poste in atto misure di sicurezza più elevate al crescere del livello di riservatezza dello stesso.
- Gli addetti di **SPI** dovranno essere formati sui corretti comportamenti da tenere per evitare attacchi da parte di software maligno (difesa da spamming, virus, ecc).
- Per nessun motivo la Casella di Posta Elettronica Istituzionale potrà essere utilizzata per scopi diversi da quelli previsti da **SPI**.

Articolo 47: Protocollazione e classificazione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- In ogni caso i documenti oggetto di classificazione e protocollazione in arrivo od in partenza non dovranno mai risiedere sulle stazioni di lavoro, ma solo sulle partizioni del server destinate all'archivio corrente.

Articolo 48: Fascicolazione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- In caso di assegnazione alla **UOR** errata, il rinvio del documento a **SPI** dovrà avvenire attraverso una casella di posta DIFFERENTE dalla Casella di Posta Elettronica Istituzionale, e con invio di ricevuta di ritorno.
- Politiche di eredità del livello di riservatezza:
 - un documento che attiene ad un fascicolo con livello di riservatezza più elevato, ne eredita il livello;
 - un documento che attiene ad un fascicolo con livello di riservatezza inferiore, mantiene invariato il suo livello.

Articolo 49: Spedizione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- Nel caso di invio di documenti cartacei, dopo aver stampato e imbustato il documento, la **UOR** provvederà in tempi brevi (di norma nello stesso giorno lavorativo della sua registrazione) alla consegna del plico chiuso a **SPI** che si incarica della spedizione.
- Nel caso di invio di documenti informatici le stazioni di lavoro della **UOR** predisposte alla spedizione di documenti dovranno essere provvisti di antivirus aggiornato come da politiche generali e il documento informatico oggetto di spedizione deve essere scrupolosamente verificato con il software antivirus prima del suo invio.

Articolo 50: Archiviazione e conservazione

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- Ferme restando le modalità generali previste dall'Art. 30 della Sez. IV, il processo di versamento delle pratiche chiuse avverrà nel seguente modo:
 - la **UOR** seleziona le pratiche chiuse da versare e le rende disponibili al prelievo copiandole dall'archivio corrente in un archivio di transito accessibile solo a **RSPI**;
 - **RSPI** o suo delegato predefinito le preleva, e le versa nell'archivio di deposito, rendendole accessibili alla **UOR** che le ha versate;
 - **RSPI** segnala alla **UOR** l'avvenuta archiviazione con la redazione di un verbale di versamento;
 - a fronte del verbale di versamento, la **UOR** ha il compito di cancellare dall'archivio corrente le pratiche versate dandone comunicazione a **SPI**.
- Almeno una volta all'anno l'archivio di deposito dovrà essere salvato in due copie su supporto non riscrivibile. Questa operazione dovrà essere svolta comunque dopo ogni versamento e dovrà essere oggetto di apposita scrittura contenente tutti i dati significativi: almeno nominativo dell'operatore, data di salvataggio ed estremi dell'ultimo versamento effettuato.
- Le copie dovranno essere conservate in idonei locali distinti. Una copia sarà conservata in locali accessibili facilmente agli addetti di **SPI** ed utilizzata per garantirne l'accesso alle **UOR** nei casi di indisponibilità del sistema di gestione informatica dei documenti, mentre l'altra che costituisce la copia di riserva sarà conservata in armadio ignifugo in altri locali a cura di **RSPI**. La copia di riserva va utilizzata solo per motivi eccezionali in caso di perita o distruzione della prima solo per il tempo necessario a ripristinare la copia utilizzata per l'accesso ai dati. Nel caso in cui l'archivio di deposito sia conservato SOLO su supporti ottici (CDROM), sarà cura dell'Amministrazione predisporre la strumentazione opportuna per fare in modo che i documenti siano comunque accessibili in tempi compatibili con le necessità del richiedente.

- I verbali di versamento sono conservati da **SPI**.
- Anche se la **UOR** mantiene i diritti di accesso sui documenti versati in deposito, la richiesta di riapertura di un fascicolo o pratica dovrà essere inoltrata a **SPI** in forma scritta.
- Per quanto attiene all'archivio storico, in caso di contratti di esternalizzazione del servizio, dovranno essere previste clausole che definiscano i livelli di servizio:
 - tempo massimo in cui il fornitore del servizio si impegna a rendere disponibile il documento richiesto;
 - impegno del fornitore del servizio a non rilasciare documenti in originale senza l'autorizzazione di **SPI**;
 - impegno del fornitore del servizio a garantire la corretta conservazione dell'archivio;
 - nel caso il fornitore del servizio renda disponibile la consultazione remota dell'archivio, dovrà provvedere alla corretta protezione dei dati in suo possesso, con gli strumenti messi a disposizione dalla tecnologia (possibilità di danni all'immagine);
 - dovranno essere previste penali per: danneggiamento degli originali, danni all'immagine derivanti da attacchi informatici, ecc.
- Nel caso l'archivio storico sia locato presso l'Amministrazione e sia possibile l'accesso remoto, dovranno essere presi opportuni provvedimenti per la protezione da attacchi esterni.
- Nell'Art. 22 della Sez. III sono indicate le modalità di realizzazione delle copie di salvataggio dell'archivio storico.

Articolo 51: Gestione dei flussi documentali

Le misure di sicurezza attinenti a questa fase di lavorazione dei documenti sono le seguenti:

- la eventuale riattribuzione del grado di riservatezza della documentazione in arrivo alla **UOR** è a carico di **RUOR**;
- la verifica del rispetto delle politiche di ereditarietà dei livelli di riservatezza dai documenti ai fascicoli di cui all'Art. 48 della Sez. VI è responsabilità di **RUOR**;
- la corretta gestione del flusso documentale è responsabilità di **RPA**. **RPA** si fa carico, in caso di gestione manuale del "workflow", della corretta esecuzione delle fasi di cancellazione dei documenti inviati ad altre **UOR**.

SEZIONE VII: Tempificazione dell'intervento

Articolo 52: Prima fase di attuazione

Nella prima fase di attuazione della normativa sul Protocollo Informatico Unico saranno garantite le funzionalità del "Nucleo Minimo" previste dall' art. 3 D.P.C.M. 31 Ottobre 2000.

Articolo 53: Seconda fase di attuazione

L'Amministrazione compatibilmente con le risorse Umane, Finanziarie e tecniche necessarie a supportare l'intera organizzazione del Protocollo, degli Archivi e dei flussi Documentali previsti dal presente Manuale di Gestione, provvederà alla complessiva applicazione dello stesso.