UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
DG/2013/1503 del 15/11/2013
Firmatari: LIGUORI Maria Luigia

Segr. D.G.

IL DIRETTORE GENERALE

VISTO l'art. 24 dello Statuto di Ateneo;

VISTO il DPR 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

VISTO il DPCM 31 ottobre 2000 e s.m.i. (Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428) ed in particolare l'art. 5, relativo al Manuale di gestione del Protocollo Informatico delle Pubbliche Amministrazioni;

VISTA la nota n.100063 del 13.11.2013, con la quale la dott.ssa Clelia Baldo, nella sua qualità di Responsabile del Servizio di Coordinamento del Protocollo Informatico, istituito con Decreto Direttoriale n.3 del 07.01.2009, ha inviato alla Direzione Generale la nuova versione (n. 1.0 del 07.10.2013) del "*Manuale di gestione del protocollo informatico, dei documenti e dell'archivio dell'Università degli Studi di Napoli Federico II*";

ESAMINATI i contenuti del predetto Manuale di gestione;

DECRETA

E' emanato il "*Manuale di gestione del protocollo informatico, dei documenti e dell'archivio dell'Università degli Studi di Napoli Federico II*", predisposto dal Responsabile del Servizio di Coordinamento del Protocollo Informatico, nella versione 1.0 del 07.10.2013, il cui testo è allegato al presente decreto per formarne parte integrante e sostanziale.

IL DIRETTORE GENERALE
Dott.ssa Maria Luigia Liguori

Ripartizione Attività di supporto istituzionale
Responsabile ad interim: dott.ssa Maria Luigia Liguori, Direttore Generale
Ufficio Segreteria di Direzione Generale
Responsabile: dott.ssa Rossella Maio, Capo dell'Ufficio
Tel: 081 2537316 – Fax: 081 2537365

UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DELL'UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

A cura del Servizio di Coordinamento del Protocollo Informatico

Versione: 1.0
Data ultima revisione: 31.10.2013

Redatto sulla base del modello di riferimento predisposto da:

AGENZIA PER L'ITALIA DIGITALE

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

INDICE

INTRODUZIONE 8

1. PRINCIPI GENERALI 9

1.1. PREMESSA 9
1.2. AMBITO DI APPLICAZIONE DEL MANUALE 10
1.3. DEFINIZIONI E NORME DI RIFERIMENTO 10
1.4. AREA ORGANIZZATIVA OMOGENEA E MODELLO ORGANIZZATIVO 11
1.5. SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO 13
1.6. CONSERVAZIONE DELLE COPIE DI RISERVA 14
1.7. FIRMA DIGITALE 14
1.8. TUTELA DEI DATI PERSONALI 14
1.9. CASELLE DI POSTA ELETTRONICA 15
1.10. SISTEMA DI CLASSIFICAZIONE DEI DOCUMENTI 16
1.11. FORMAZIONE 17
1.12. ACCREDITAMENTO DELL'AMMINISTRAZIONE ALL'IPA 18
1.13. PROCEDURE INTEGRATIVE DI CONSERVAZIONE SOSTITUTIVA 19
1.14. IL SITO WEB PER L'EGOVERNMENT 19

2. ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO 20

2.1. PIANO DI ATTUAZIONE 20
2.2. GLI OBIETTIVI OPERATIVI 20

3. PIANO DI SICUREZZA 23

3.1. OBIETTIVI DEL PIANO DI SICUREZZA 23
3.2. GENERALITÀ 23
3.3. FORMAZIONE INFORMATICA DEI DOCUMENTI – ASPETTI DI SICUREZZA 25
3.4. GESTIONE INFORMATICA DEI DOCUMENTI – ASPETTI DI SICUREZZA 26
3.5. POLITICHE DI SICUREZZA ADOTTATE DALLA AOO 27

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI 29

4.1. IL DOCUMENTO INFORMATICO 29
4.2. IL DOCUMENTO ANALOGICO - CARTACEO 31
4.3. FORMAZIONE DEI DOCUMENTI – ASPETTI OPERATIVI 31
4.4. SOTTOSCRIZIONE DI DOCUMENTI INFORMATICI 32
4.5. APPOSIZIONE DELLA FIRMA DIGITALE 32
4.6. VERIFICA DELLE FIRME CON IL PDP 33
4.7. REQUISITI DEGLI STRUMENTI INFORMATICI DI SCAMBIO 33
4.8. DOCUMENTO RICEVUTO DALLA AOO ("ENTRATA") 34
4.9. DOCUMENTO INVIATO DALLA AOO ("USCITA") 34
4.10. DOCUMENTO INTERNO FORMALE ("TRA UFFICI") 35
4.11. DOCUMENTO INTERNO INFORMALE 35
4.12. USO DELLA POSTA ELETTRONICA CERTIFICATA 35

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI 39

5.1. GENERALITÀ 39
5.2. FLUSSO DEI DOCUMENTI RICEVUTI 39
5.2.1. Flusso documenti cartacei "Entrata" 39

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

5.2.2. Flusso documenti informatici in "Entrata" ... *43*
5.2.3. Flusso di documenti interni formali ("Tra Uffici") ... *44*
5.2.4. Ricezione di documenti informatici sulla casella di posta istituzionale ... *47*
5.2.5. Ricezione di documenti informatici sulla casella di posta elettronica certificata non istituzionale ... *47*
5.2.6. Ricezione di documenti informatici su supporti rimovibili ... *48*
5.2.7. Ricezione di documenti cartacei a mezzo posta convenzionale ... *48*
5.2.8. Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali ... *48*
5.2.9. Errata ricezione di documenti digitali ... *48*
5.2.10. Errata ricezione di documenti cartacei ... *48*
5.2.11. Attività di protocollazione dei documenti ... *49*
5.2.12. Rilascio di ricevute attestanti la ricezione di documenti informatici ... *49*
5.2.13. Rilascio di ricevute attestanti la ricezione di documenti cartacei ... *50*
5.2.14. Archiviazione dei documenti informatici ... *50*
5.2.15. Archiviazione delle rappresentazioni digitali di documenti cartacei ... *50*
5.2.16. Classificazione, assegnazione e presa in carico dei documenti ... *51*
5.2.17. Conservazione dei documenti nell'archivio corrente ... *51*
5.2.18. Conservazione dei documenti e dei fascicoli nella fase corrente ... *52*
5.3. FLUSSO DOCUMENTI INVIATI DALLA AOO ... 52
5.3.1. Sorgente interna dei documenti ... *56*
5.3.2. Verifica formale dei documenti ... *56*
5.3.3. Registrazione di protocollo e segnatura ... *56*
5.3.4. Trasmissione di documenti informatici ... *57*
5.3.5. Trasmissione di documenti cartacei a mezzo posta ... *58*
5.3.6. Affrancatura dei documenti in partenza ... *58*
5.3.7. Conteggi spedizione corrispondenza ... *58*
5.3.8. Documenti in partenza per posta convenzionale con più destinatari ... *58*
5.3.9. Trasmissione di documenti cartacei a mezzo telefax ... *58*
5.3.10. Inserimento delle ricevute di trasmissione nel fascicolo ... *58*

6. REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI 60

6.1. REGOLE DISPONIBILI CON IL PDP ... 60
6.2. CORRISPONDENZA DI PARTICOLARE RILEVANZA ... 61
6.3. ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO DIGITALE ... 61
6.4. ASSEGNAZIONE DEI DOCUMENTI RICEVUTI IN FORMATO CARTACEO ... 61
6.5. MODIFICA DELLE ASSEGNAZIONI ... 62

7. UO RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI.....64

7.1. SERVIZIO DI PROTOCOLLO ... 64
7.2. SERVIZIO ARCHIVISTICO ... 65
7.3. SERVIZIO DI COORDINAMENTO DEL PROTOCOLLO INFORMATICO ... 65
7.4. SERVIZIO DELLA CONSERVAZIONE ELETTRONICA DEI DOCUMENTI ... 67
7.4.1. Archiviazione ottica dei documenti analogici ... *67*
7.4.2. Archiviazione ottica dei documenti digitali ... *67*

8. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO 69

8.1. DOCUMENTI ESCLUSI ... 69
8.2. DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE ... 69
8.3. NORME DI UTILIZZO DEL PROTOCOLLO PARTICOLARE ... 70
8.3.1. La registrazione di protocollo ... *70*
8.3.2. Acquisizione dell'immagine del documento ... *70*

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

8.3.3. Stampa e tenuta del registro particolare 70
8.3.4. Annullamento di registrazioni di protocollo particolare 71
8.3.5. Abilitazione all'accesso a dati e funzioni 71

9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE 72

9.1. PROTEZIONE E CONSERVAZIONE DEGLI ARCHIVI PUBBLICI 72
9.1.1. Generalità 72
9.1.2. Misure di protezione e conservazione degli archivi pubblici 73
9.2. TITOLARIO O PIANO DI CLASSIFICAZIONE 73
9.2.1. Titolario 73
9.2.2. Classificazione dei documenti 74
9.3. FASCICOLI ELETTRONICI 75
9.3.1. Fascicolazione dei documenti 75
9.3.2. Apertura del fascicolo 75
9.3.3. Chiusura del fascicolo 75
9.3.4. Processo di assegnazione dei fascicoli 76
9.3.5. Modifica delle assegnazione dei fascicoli 76
9.3.6. Repertorio dei fascicoli 77
9.4. SERIE ARCHIVISTICHE E REPERTORI 77
9.4.1. Serie archivistiche 77
9.4.2. Repertori e serie archivistiche 78
9.4.3. Versamento dei fascicoli nell'archivio di deposito 79
9.4.4. Verifica della consistenza del materiale riversato nell'archivio di deposito 80
9.5. SCARTO, SELEZIONE E RIORDINO DEI DOCUMENTI 81
9.5.1. Operazione di scarto 81
9.5.2. Conservazione del materiale presso la sezione di deposito dell'archivio 82
9.5.3. Versamento dei documenti nella sezione separata dell'archivio di deposito o generale: sezione detta "archivio storico". 82
9.6. CONSULTAZIONE E MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO E STORICO 82
9.6.1. Principi generali 82
9.6.2. Consultazione ai fini giuridico-amministrativi 82
9.6.3. Consultazione per scopi storici 82
9.6.4. Consultazione da parte di personale esterno all'Amministrazione: 83
9.6.5. Consultazione da parte di personale interno all'Amministrazione 84
9.6.6. Schematizzazione del flusso dei documenti all'interno del sistema archivistico 84

10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO 86

10.1. UNICITÀ DEL PROTOCOLLO INFORMATICO 86
10.2. REGISTRO GIORNALIERO DI PROTOCOLLO 87
10.3. REGISTRAZIONE DI PROTOCOLLO 87
10.3.1. Documenti informatici 87
10.3.2. Documenti analogici (cartacei e supporti rimovibili) 89
10.4. ELEMENTI FACOLTATIVI DELLE REGISTRAZIONI DI PROTOCOLLO 90
10.5. SEGNATURA DI PROTOCOLLO DEI DOCUMENTI 90
10.5.1. Documenti informatici 91
10.5.2. Documenti cartacei 93
10.6. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO 93
10.7. LIVELLO DI RISERVATEZZA 94
10.8. CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO 95
10.8.1. Registrazioni di protocollo particolari 95
10.8.2. Circolari e disposizioni generali 95
10.8.3. Documenti cartacei in partenza con più destinatari 96

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.8.4. Documenti cartacei ricevuti a mezzo telegramma ... 96
10.8.5. Documenti cartacei ricevuti a mezzo telefax ... 96
10.8.6. Protocollazione di un numero consistente di documenti cartacei ... 97
10.8.7. Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio ... 97
10.8.8. Fatture, assegni e altri valori di debito o credito ... 97
10.8.9. Protocollazione di documenti inerenti a gare di appalto confezionate su supporti cartacei 98
10.8.10. Protocolli urgenti ... 98
10.8.11. Documenti non firmati ... 98
10.8.12. Protocollazione dei messaggi di posta elettronica convenzionale ... 99
10.8.13. Protocollo di documenti digitali pervenuti erroneamente ... 99
10.8.14. Ricezione di documenti cartacei pervenuti erroneamente ... 99
10.8.15. Copie per conoscenza ... 99
10.8.16. Differimento delle registrazioni ... 99
10.8.17. Registrazioni di documenti temporaneamente riservati ... 101
10.8.18. Corrispondenza personale o riservata ... 101
10.8.19. Integrazioni documentarie ... 102
10.9. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO CON IL PDP ... 102
10.10. REGISTRAZIONI DI PROTOCOLLO ... 102
10.10.1. Attribuzione del protocollo ... 102
10.10.2. Registro informatico di protocollo ... 103
10.10.3. Tenuta delle copie del registro di protocollo ... 104

11. DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO ... 105

11.1. DESCRIZIONE FUNZIONALE ED OPERATIVA ... 105
11.1.1. La soluzione adottata dall'Università ... 105
11.1.2. Le funzionalità dell'applicazione E-Grammata ... 105
11.1.2.1 Le funzionalità generali ... 105
11.1.2.2 Le funzionalità di gestione dati di profilazione ... 107
11.1.2.3 Le funzionalità di sicurezza ... 109
11.1.2.4 Le funzionalità per la gestione documentale ... 110
11.1.2.5 Le funzionalità per la gestione del lavoro cooperativo ed interoperabilità ... 110
11.1.2.6 Stampe e demone di stampa ... 112
11.1.2.7 Le funzioni crittografiche ... 112
11.2. L'ARCHITETTURA APPLICATIVA ... 112
11.3. L'ACQUISIZIONE MASSIVA DEI DOCUMENTI ANALOGICI ... 113

12. RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI ... 117

12.1. GENERALITÀ ... 117
12.2. ABILITAZIONI INTERNE AD ACCEDERE AI SERVIZI DI PROTOCOLLO ... 117
12.3. PROFILI DI ACCESSO ... 118
12.3.1 Il conferimento delle abilitazioni ... 118
12.3.2 Utente amministratore di PdP ... 119
12.3.3 I profili utente ... 119
12.4. MODALITÀ DI CREAZIONE E GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO ... 120
12.5. ABILITAZIONI ESTERNE (PRIVATI) ... 121
12.6. ABILITAZIONI ESTERNE CONCESSE AD ALTRE AOO ... 121
12.7. CONSULTAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO PARTICOLARI ... 122

13. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA ... 123

13.1. IL REGISTRO DI EMERGENZA ... 123
13.2. MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA ... 124
13.3. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA ... 125

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

13.4. MODALITÀ DI CHIUSURA E RECUPERO DEL REGISTRO DI EMERGENZA 125
13.5. MODALITÀ DI COMPLETAMENTO DELLE REGISTRAZIONI DI EMERGENZA 126
13.6. IL REGISTRO DEI PROTOCOLLI DI EMERGENZA 127

14. GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI 128

14.1. MATRICE DELLE CORRELAZIONI 128
14.2. CATALOGO DEI PROCEDIMENTI AMMINISTRATIVI 128
14.3. AVVIO DEI PROCEDIMENTI E GESTIONE DEGLI STATI DI AVANZAMENTO 129

15. AGGIORNAMENTO DEL MANUALE 130

15.1. MODALITÀ DI AGGIORNAMENTO E APPROVAZIONE DEL MANUALE 130
15.2. PUBBLICITÀ DEL PRESENTE MANUALE 130

ALLEGATI 131

INDICE DEGLI ALLEGATI 132

A1. DEFINIZIONI 134

A2. NORMATIVA DI RIFERIMENTO 146

A2.1. LEGGI E NORME 146
A2.2. REGOLAMENTI E ATTI DELL'ATENEO 148

A3. AREA ORGANIZZATIVA OMOGENEA E CARATTERISTICHE ORGANIZZATIVE 151

A3.1. DATI IDENTIFICATIVI DELL'AMMINISTRAZIONE 151
A3.2. CARATTERIZZAZIONE DELL'AREA ORGANIZZATIVA OMOGENEA 151
A3.3. ORGANIGRAMMA DEL PROTOCOLLO INFORMATICO 152
A3.4. UOR E RELATIVI CODICI DI REGISTRO EMERGENZA 158

A4. ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO DI COORDINAMENTO DEL PROTOCOLLO INFORMATICO 162

A5. I TITOLARI DI FIRMA DIGITALE 166

A6. PIANO FORMATIVO PER IL PERSONALE DELL'AMMINISTRAZIONE PER L'AVVIO DEL SISTEMA 167

A6.1. I MODULI FORMATIVI 167
A6.2. I PROFILI DEI FRUITORI DEI CORSI 168
A6.3. I PERCORSI FORMATIVI 169
A6.4. DETTAGLIO DEL CONTENUTO DEI CORSI 170

A7. PIANO DI ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO 173

A8. MISURE DI SICUREZZA 180

A8.1. L'ARCHITETTURA TECNICA DEL SISTEMA 180
A8.2. L'ARCHITETTURA APPLICATIVA 181

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A8.3. L'ARCHITETTURA DI SICUREZZA 182
Le funzioni di sicurezza *182*
A8.3.1. Descrizione generale dei meccanismi di sicurezza implementati nel PdP *184*
A8.3.2. Le funzioni di sicurezza di tipo informatico *186*
A8.3.3. Componente organizzativa della sicurezza *196*
A8.3.4. Componente infrastrutturale della sicurezza *199*
A8.3.5. Le minacce e gli agenti *201*
A8.3.6. La tabella di correlazione minacce/funzioni di sicurezza *202*
A8.3.7. Determinazione del grado di copertura e del rischio residuo *204*

A9. CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO 206

A10. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO 209

A10.1. DOCUMENTI IN ARRIVO 209
A10.2. DOCUMENTI IN PARTENZA 210
A10.3. DOCUMENTI INTERNI 210
A10.4. ECCEZIONI 210

A11. ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE 211

A12. TITOLARIO DI CLASSIFICAZIONE 212

A13. REPERTORI GENERALI 216

A14. ELEMENTI DELLA SEGNATURA DI PROTOCOLLO PER LA CORRISPONDENZA CARTACEA 217

A14.1 ESEMPIO DI SEGNATURA PRODOTTA DAGLI SCANNER MASSIVI 217
A14.2 ESEMPIO DI SEGNATURA PRODOTTA DAGLI SCANNER PRESSO LE UOR DIVERSE DALL'AMMINISTRAZIONE CENTRALE 217
A14.3 IL TIMBRO DIGITALE 218

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

INTRODUZIONE

Il presente Manuale di gestione del protocollo informatico, dei documenti e dell'archivio dell'Università degli Studi di Napoli Federico II, redatto nella sua prima edizione 'integrale" nel corso del 2013, raccoglie l'insieme dei decreti, degli atti, delle comunicazioni, dei documenti tecnici ed amministrativi, dei manuali e delle guide operative che negli anni hanno costituito l'insieme delle politiche e delle prassi operative adottate dall'Ateneo in materia di gestione e di tenuta dei flussi documentali informatici. Tale patrimonio informativo, pubblicato e reso disponibile all'indirizzo www.praxis.unina.it, è stato quindi unificato, integrato ed aggiornato, anche in funzione dei recenti e strutturali cambiamenti organizzativi dell'Ateneo, oltre che dell'attuale quadro normativo di riferimento.

L'obiettivo è l'emanazione e la messa a disposizione di tutto il personale e dei cittadini, nel formato standard proposto dall'Agenzia per l'Italia Digitale, di un documento di riferimento che illustri - in modo integrato e coerente - le scelte tecnico-organizzative operate negli anni dall'Università per la gestione ed il trattamento dei flussi dei documenti amministrativi informatici, con particolare riguardo al loro processo di formazione, classificazione, fascicolazione, registrazione di protocollo, assegnazione, gestione dell'iter, trasmissione e archiviazione informatica. Il documento non ha pretesa di completezza. Al contrario, rappresenta una prima base di sistematizzazione della materia e si raccorderà e completerà con gli altri documenti programmatici che saranno redatti nei mesi a seguire dai rispettivi responsabili: dai Manuali di conservazione dei documenti informatici e dei documenti analogici, al Massimario di scarto dei documenti amministrativi, al Catalogo dei procedimenti amministrativi.

Pertanto, negli anni a venire, il presente Manuale sarà sottoposto ad un processo di revisione, arricchimento ed aggiornamento continuo, in modo tale da risultare sempre più adeguato a descrivere un sistema, quello documentale, in continuo cambiamento sia per gli aspetti organizzativi che normativi che tecnologici.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1. PRINCIPI GENERALI

1.1. Premessa

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

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DPR n. 428 del 20 ottobre 1998)".

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione. Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.
Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.
Esso disciplina:

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

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

1.2. Ambito di applicazione del manuale

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, recante le regole tecniche per il protocollo informatico.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'**Università degli Studi di Napoli Federico II** a partire dal **1 gennaio 2007**, data di costituzione dell'Area Organizzativa Omogenea e di avvio del sistema di Protocollo Generale di Ateneo.

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

Il protocollo, inoltre, fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intende:

- per "Amministrazione", l'Università degli Studi di Napoli Federico II;
- per "Testo Unico", il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- per "Codice", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'Amministrazione digitale.

Per le definizioni vedasi l'elenco riportato nell'**allegato 1**.

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

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico, dei documenti e degli archivi;
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **PdP -** Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'Amministrazione per implementare il servizio di protocollo informatico. Nel caso dell'Università è l'applicativo eGrammata;
- **RSI** - Responsabile del Servizio Informatico per la gestione del protocollo, dei flussi documentali e dell'archiviazione elettronica. Nel caso dell'Università, coincide con il Centro Servizi Informativi di Ateneo (C.S.I.);
- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema di protocollo informatico; ovvero il soggetto destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le Norme e i Regolamenti di riferimento vedasi l'elenco riportato nell'**allegato 2** .

1.4. Area Organizzativa Omogenea e modello organizzativo

La scelta operata dall'Ateneo è stata di configurarsi, ai fini della gestione documentale, come unica Area Organizzativa Omogenea denominata "Università degli Studi di Napoli Federico II", di seguito AOO, composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato nell'**allegato 3** e di definire, quindi, un registro di protocollo generale, unico per tutte le proprie strutture. Di seguito, si riporta una tabella in cui si evidenziano i vantaggi derivanti da tale scelta organizzativa:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Caratteristica	Vantaggi
Unicità del Registro di protocollo	▪ Riduzione della frammentazione ▪ Riduzione del numero di registrazioni di protocollo ▪ Maggiore flessibilità del servizio ▪ Indipendenza dalle dinamiche di riorganizzazione dell'Ateneo ▪ Standardizzazione (es. titolario di classificazione) ▪ Maggiore coesione tra le strutture
Unicità dell'archivio elettronico contenente i documenti protocollati	▪ Riduzione della ridondanza della documentazione da gestire ▪ Semplificazione delle operazioni di reperimento dei documenti
Unicità del Manuale di Gestione	▪ Omogeneità di organizzazione del servizio ▪ Riduzione dei costi di gestione del servizio
Flussi interni di tipo "intra-AOO"	▪ Semplificazione dell'iter documentale ▪ Snellimento dei procedimenti amministrativi

Nell'allegato 3 sono inoltre riportati la denominazione, il codice identificativo dell'Amministrazione e l'insieme delle UOR che la compongono con la loro articolazione in UU.

All'interno dell'Amministrazione il sistema di protocollazione è unico e totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto ogni UOR svolge anche i compiti di UOP. Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del RSP.

L'allegato 3 è suscettibile di modifica in caso di inserimento di nuove UOR/UU o di riorganizzazione delle medesime.

Le modifiche all'organigramma del sistema del protocollo informatico sono recepite da RSP in funzione di variazioni derivanti da istituzioni o cessazioni di strutture, ratificate da decreti rettoriali o direttoriali. L'Amministrazione si riserva altresì la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altre UOR allo svolgimento dell'attività di protocollazione e/o di gestione dei flussi documentali.

In tutte le UOR è utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione è abilitato dal RSI sulla base della richiesta comunicata (mediante utilizzo del modello SICURDAT/B, come sarà dettagliatamente descritto nel seguito del documento) dal Responsabile UOR/UU alla Direzione Generale e da quest'ultima autorizzata. L'RSP ha anche il compito di vigilare sulla corretta esecuzione delle attività.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1.5. Servizio per la gestione informatica del protocollo

Con decreto DD n.3 del 7.1.2009, nell'AOO precedentemente individuata è stato istituito a decorrere dal 7.1.2009, ai sensi all'art. 61 del succitato D.P.R. 445/2000, il "Servizio di Coordinamento del Protocollo Informatico" per la gestione informatica dei documenti, dei flussi documentali e degli archivi. Al "Servizio di Coordinamento del Protocollo Informatico" vengono attribuite le seguenti specifiche competenze:

- Interviene su tutte le UOR dell'Ateneo di cui in premessa, nel rispetto della autonomia operativa di ciascuna struttura, con funzione di coordinamento, monitoraggio e controllo in merito agli adempimenti connessi con la procedura del protocollo informatico e di gestione dei flussi documentali;
- Garantisce che il sistema informatico consenta lo svolgimento delle operazioni di registrazione e di segnatura di protocollo in ottemperanza con quanto stabilito dalla legislazione vigente in materia;
- Attiva il Centro Servizi Informativi d'Ateneo (C.S.I.) affinché le funzionalità del sistema, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile, coerentemente con livelli di servizio preventivamente concordati e, comunque entro le ventiquattro ore dal blocco delle attività;
- Stabilisce con il C.S.I. le procedure per la corretta produzione e conservazione del registro giornaliero di protocollo e per la conservazione delle copie di salvataggio delle informazioni del sistema e vigila sull'osservanza di quanto concordato;
- Definisce i profili di abilitazione (ruoli) per l'accesso alle funzioni ed ai dati del sistema di Protocollo Informatico che i responsabili di U.O.R. attribuiscono ai propri incaricati;
- Propone i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, e, più in generale, dei protocolli diversi dal protocollo informatico;
- Fornisce consulenza alle strutture in materia per quanto attiene alla attuazione delle politiche di gestione informatica dei documenti, dei fascicoli ed dei flussi documentali;
- Predispone lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo e ne cura l'aggiornamento;
- Provvede alla pubblicazione del manuale anche per via telematica;
- Predispone il piano per la sicurezza informatica relativo alla protezione della integrità, della riservatezza e della disponibilità dei documenti e delle informazioni trattate nell'ambito del sistema di Protocollo Informatico e di gestione dei flussi documentali, d'intesa con il C.S.I. ed il titolare dei trattamenti dei dati di cui al dlgs. n. 196/2003 "Codice in materia di protezione dei dati personali";
- Garantisce l'adeguatezza degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e di gestione informatica degli archivi elettronici;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Aggiorna il Titolario di classificazione, sulla base delle indicazioni fornite dalle U.O.R;
- Cura, d'intesa con i responsabili degli uffici preposti alla gestione degli archivi, la definizione dei requisiti del sistema di conservazione a norma dei documenti cartacei.

Il Servizio è istituito nell'ambito dell'Area Tecnica "e-Government" del C.S.I. e si avvale della collaborazione delle Aree Tecniche del C.S.I. e dell'Ufficio Protocollo e dell'Ufficio Archivio dell'Amministrazione Centrale, nonché delle UOR e dei rispettivi UOP.

Responsabile del servizio "Servizio di Coordinamento del Protocollo Informatico" è il Direttore dell'Area Tecnica "e-Government" del C.S.I., che risponde direttamente al Direttore Generale.

L'atto che istituisce il servizio è riportato nell'**allegato 4**.

1.6. Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, **il contenuto del registro informatico di protocollo** viene estratto al termine di ogni giornata, salvato in formato pdf e quindi in automatico registrato nel sistema di protocollo, i modo tale da garantirne la immodificabilità. Tale documento, al pari di tutti i restanti oggetti registrati nel sistema di Protocollo Informatico, è sottoposto alle procedure di salvataggio predisposte da RSI, illustrate nel piano di sicurezza contenuto nel presente MdG.

1.7. Firma digitale

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'Amministrazione fornisce la firma digitale ai soggetti da essa delegati a rappresentarla. Ai sensi del Regolamento di Ateneo in materia di firma digitale, i documenti amministrativi sottoscritti con firma digitale devono essere sottoposti a registrazione di protocollo. Il documento registrato nel sistema di protocollo rappresenta il documento originale. All'atto della registrazione, il sistema verifica l'autenticità ed integrità del documento e ne registra, in modo immodificabile, la data e l'ora di protocollazione e l'esito dei controlli di autenticità ed integrità del documento, come illustrato più dettagliatamente nel paragrafo 10.3.1.

1.8. Tutela dei dati personali

L'amministrazione titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna. Più in dettaglio:

- Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal rispettivo responsabile nominato dal titolare del trattamento dei dati e da questi formalmente autorizzati.
- Relativamente agli adempimenti esterni, l'Amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

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

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

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

1.9. Caselle di Posta Elettronica

L'Ateneo, **gestore pubblico PEC iscritto dal 30.09.2009 al registro IGPEC dei gestori accreditati**, si è dotato della casella di posta elettronica certificata istituzionale "**ateneo@pec.unina.it**" per la corrispondenza, sia in ingresso che in uscita della AOO. Tale indirizzo è pubblicato sull'Indice delle Pubbliche Amministrazioni (**IPA**) e costituisce l'indirizzo virtuale dell'Amministrazione e di tutti gli uffici (UOR) che ad essa fanno riferimento.

Sono inoltre dotate di casella PEC: la Direzione Generale, le Ripartizioni, gli Uffici e le altre strutture dell'Università (Dipartimenti, Scuole, Centri, Biblioteche, etc.). Di questi indirizzi sono stati ad oggi pubblicati in IPA, come si dirà più diffusamente nel paragrafo 1.12, oltre all'indirizzo istituzionale, anche quello delle Ripartizioni e dei Dipartimenti,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

in modo tale da consentire la interoperabilità anche con l'infrastruttura "CEC-PAC" resa disponibile ai cittadini dal Ministero per la pubblica amministrazione e l'innovazione.

Sono titolari delle caselle PEC delle strutture i responsabili pro-tempore delle stesse che per la gestione operativa delle stesse si possono avvalere di incaricati autorizzati.

In corrispondenza di ciascuna casella PEC, le strutture dispongono anche di una casella di posta elettronica di tipo tradizionale, destinata – tra l'altro – a raccogliere tutti messaggi di posta elettronica *con annessi documenti ed eventuali allegati* destinati ad essere formalmente inviati via PEC.

Tutti gli indirizzi di PEC assegnati alle strutture, il Regolamento di Ateneo in materia di Posta Elettronica Certificata, il Manuale operativo, la modulistica e d altre informazioni utili ai fini dell'utilizzo del servizio UNINAPEC sono disponibili all'indirizzo: **http://www.unina.it/UNINAPEC**.

Infine, in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per la pubblica amministrazione e l'innovazione sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione dota tutti i propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, di una casella di posta elettronica e, a partire dal 7 agosto 2013, assegna una casella PEC a tutto il personale docente e ricercatore, anche a tempo determinato.

1.10. Sistema di classificazione dei documenti

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

Il "Testo unico" sancisce – tra l'altro – che per la tenuta del sistema informativo automatizzato finalizzato alla gestione del protocollo informatico e dei procedimenti amministrativi, oltre alle operazioni di registrazione e di segnatura di protocollo, è necessaria anche quella di classificazione dei documenti, effettuata sulla base di un adeguato piano di classificazione d'archivio (o titolario) definito da ciascuna amministrazione. In questo modo, il sistema di gestione del protocollo informatico e dei procedimenti amministrativi può fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato e consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Il piano di classificazione è quindi uno schema logico per organizzare i documenti d'archivio, è uno strumento di ordinamento ed organizzazione funzionale dei documenti che ne consente il facile reperimento, la soggettazione e l'indicizzazione. Mediante il piano di classificazione, è inoltre possibile recuperare e consultare l'archivio secondo le modalità stesse in cui i documenti sono stati ordinati nel corso del quotidiano lavoro amministrativo. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente; le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella funzione descritta dal titolo, secondo un'articolazione gerarchica.

L'Amministrazione, in accordo con le prescrizioni normative sopra richiamate, il 1° gennaio 2007 ha istituito il Protocollo Generale di Ateneo e contestualmente ha avviato l'esercizio del sistema di Protocollo Informatico utilizzando, **in via transitoria**, il Titolario adottato nel 2000 dalla sola Amministrazione Centrale. A seguire, ha quindi operato la revisione del Titolario stesso, per adeguarlo al quadro normativo vigente e alla struttura organizzativa dell'Ateneo e per renderlo idoneo a soddisfare le esigenze di classificazione dei documenti di tutte le strutture dell'Ateneo. **L'Amministrazione, con** OdS n. 159 del 3 giugno 2008, ha quindi adottato il proprio Titolario di classificazione**, disponendone l'attivazione a far data dal 4 giugno 2008, nell'ambito del sistema di Protocollo Informatico.**

Al fine di facilitare l'individuazione e l'assegnazione a ciascun documento del codice di titolazione corretto, RSP ha provveduto alla predisposizione ed alla pubblicazione all'indirizzo http://www.praxis.unina.it, nella sezione "Protocollo Informatico" del "thesaurus" contenente la descrizione di ciascun titolo/classe con un sintetico riepilogo dei contenuti di ciascuna voce di titolazione ed esempi di classificazione di alcuni tra i più rilevanti procedimenti amministrativi.

Il contenuto della classificazione è dettagliatamente illustrato nel successivo capitolo 9 e nell'**allegato 12** ne è riportata l'attuale struttura.

1.11. Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro della funzione pubblica sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'Amministrazione ha stabilito percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

In particolare, considerato che il personale assegnato agli UOP deve conoscere:

- l'organizzazione ed i compiti svolti da ciascun UOR/UU all'interno dell'Amministrazione;
- gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

sono stati previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

- ai processi di semplificazione ed alle innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti dell'Amministrazione;
- agli strumenti e alle tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione;
- alle norme sulla protezione dei dati personali e alle direttive impartite dal Titolare dei dati personali trattati dall'Università.

Tali iniziative formative, destinate a specialisti, funzionari e dirigenti sono riportate nell'**allegato 6**.

1.12. Accreditamento dell'Amministrazione all'IPA

L'Amministrazione si è dotata di una casella di posta elettronica istituzionale (come già detto in precedenza, la casella ateneo@pec.unina.it) attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità dell'Ufficio di Segreteria del Direttore Generale che procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

Il Direttore Generale ha incaricato RSP di accreditare l'Amministrazione presso l'Indice delle Pubbliche Amministrazioni (IPA) e di provvedere all'inserimento ed aggiornamento sul sito tenuto e reso pubblico dall'Agenzia per l'Italia digitale (ex CNIPA, ovvero DigitPA), delle seguenti informazioni relative all'Ateneo:

- la denominazione della Amministrazione;
- il codice identificativo proposto per la Amministrazione;
- l'indirizzo della sede principale della Amministrazione;
- le informazioni relative all'Area Organizzativa Omogenea:
  - denominazione
  - casella di posta elettronica;
  - nominativo del RSP;
  - data di istituzione;
  - eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'Amministrazione.

Con particolare riguardo all'ultimo punto, alla data sono state inserite in IPA le informazioni relative alle Ripartizioni in cui si articola l'Amministrazione Centrale dell'Ateneo e quelle relative ai Dipartimenti, in accordo con quanto riportato nell'allegato 3.

Il codice identificativo della Amministrazione associato a ciascuna delle proprie AOO e UOR è stato generato ed attribuito autonomamente dall'Amministrazione.
L'IPA è accessibile tramite relativo sito internet da parte di tutti i soggetti pubblici o

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

1.13. Procedure integrative di conservazione sostitutiva

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'Amministrazione intende uniformarsi alle modalità previste dalla Codice dell'Amministrazione Digitale e dalla deliberazione CNIPA n. 11/2004. Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'Amministrazione comunica all'Agenzia per l'Italia digitale le procedure integrative che intende adottare ai sensi dell'art. 7 della citata deliberazione.

1.14. Il sito WEB per l'eGovernment

Maggiori dettagli ed informazioni sugli argomenti sopra descritti sono disponibili sul sito **http://www.praxis.unina.it** dell'Università, in cui vengono messi a disposizione dell'utente normative, regolamenti interni, manuali, guide operative e strumenti software di utilità. Realizzato con l'obiettivo di dare ordine alle informazioni creando specifiche sezioni tematiche riguardanti l'eGovernment, il protocollo informatico, la firma digitale, la posta elettronica certificata, nonché una sezione con i collegamenti rapidi alle procedure informatiche, il sito è stato sviluppato in ottemperanza con la normativa vigente in materia di accessibilità.

Le news inserite per data di pubblicazione e per canale tematico, il motore di ricerca interno dotato di funzionalità avanzate per la limitazione delle ricerche a singoli argomenti o sezioni, la mappa del sito aggiornata in tempo reale ad ogni inserimento di nuove voci nel menu di navigazione, la generazione dei percorsi a "briciole di pane" (sequenza di link) che informano costantemente il navigatore in quale punto del sito si trova, sono solo alcune delle funzionalità offerte dal sito www.praxis.unina.it.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

2. ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

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

2.1. Piano di attuazione

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'Amministrazione sono registrati all'interno del registro di protocollo informatico. Pertanto, **tutti i registri particolari di protocollo sono stati progressivamente aboliti ed eliminati**.

Per raggiungere l'obiettivo di eliminare i diversi protocolli di settore, di reparto e multipli e di dematerializzare i documenti amministrativi scambiati tra le strutture dell'Ateneo e tra l'Ateneo ed Enti esterni dotati di Protocollo Informatico a norma, nonché di snellire e ottimizzare la comunicazione interna e l'organizzazione degli Uffici dell'Amministrazione Centrale, è stato definito un **piano di attuazione del Protocollo informatico**. A tal fine, sono state svolte le seguenti attività:

- censimento preliminare dei diversi protocolli esistenti;
- analisi dei livelli di automazione;
- definizione degli interventi organizzativi procedurali e tecnici da effettuare per adottare il protocollo informatico;
- valutazione dei tempi di sostituzione;
- stima dei costi derivanti.

Le informazioni raccolte ed il piano di azione che ne è derivato tengono conto della realtà organizzativa della AOO e della necessità di gestire la fase transitoria connessa con l'esaurimento delle pratiche in essere, protocollate e gestite anteriormente all'arrivo del sistema di protocollo informatico e gestione documentale di cui al presente MdG, nonché alla necessità di procedere ad una diffusione graduale del nuovo sistema. Il piano si articola quindi in più passi, secondo un approccio incrementale, in cui ciascun passo concorre al perseguimento di un prefissato obiettivo di miglioramento ed è realizzato mediante azioni di tipo organizzativo e di tipo tecnico. Il risultato finale perseguito, che consiste nella realizzazione di un'architettura integrata di servizi, non può infatti prescindere da un'attenta sincronizzazione - sostenibile - tra la messa in campo di nuove soluzioni organizzative e tecnologiche, dove le prime sono volte alla individuazione ed alla ratifica di nuove e chiare regole, di ruoli e di responsabilità, le seconde, all'implementazione di strumenti fruibili ed altamente disponibili.

2.2. Gli obiettivi operativi

Di seguito, la sintetica descrizione degli obiettivi individuati come prioritari nel

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

predetto piano attuativo. L'elenco, per ciascun obiettivo, delle azioni di dettaglio è riportato in **allegato 7**, insieme al cronoprogramma degli interventi.

Obiettivo 0: Istituzione del Protocollo Generale ed avvio del sistema presso l'Amministrazione centrale e le strutture pilota.

Fase 1 Ricognizione della situazione. Analisi e individuazione della nuova architettura di servizio. Individuazione delle strutture pilota.

Fase 2 Acquisizione, personalizzazione e configurazione dell'applicazione informatica.

Fase 3 Formazione utenti pilota ed avvio dell'esercizio.

Obiettivo 1: Unificazione dei registri di protocollo delle strutture decentrate nel Protocollo Generale di Ateneo.

Fase 1 Acquisizione e distribuzione apparecchiature per attrezzare le postazioni di lavoro.

Fase 2 Formazione degli utenti.

Fase 3 Avvio progressivo delle strutture secondo una pianificazione di dettaglio.

Obiettivo 2 - Riduzione del flusso cartaceo (per i documenti in ingresso alla Amministrazione Centrale) tra la Direzione Generale e gli Uffici dell'Amministrazione Centrale assegnatari.

Fase 1 Ampliamento delle funzionalità del Protocollo Informatico, in modo da consentire la gestione del workflow dell'iter documentale.

Fase 2 Diffusione del Protocollo Informatico agli Uffici dell'Amministrazione Centrale.

Fase 3 Organizzazione del processo di sigla presso la Direzione Generale e le Ripartizioni.

Obiettivo 3 - Riduzione del flusso cartaceo tra le strutture dell'Ateneo.

Fase 1 Eliminazione della minuta. Il documento originale, dopo la registrazione di protocollo, viene custodito dal mittente (solo flusso interno).

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Fase 2 Diffusione della firma digitale ai Responsabili delle strutture.

Obiettivo 4 – Snellimento del carico di lavoro dell'Ufficio di Protocollo dell'Amministrazione Centrale.

Obiettivo 5 – Digitalizzazione dei procedimenti amministrativi rilevanti e avvio interoperabilità.

Il RSP esegue comunque, periodicamente, dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli sul PdP, la validità dei criteri di classificazione utilizzati e a sensibilizzare, nel caso in cui siano riscontrate anomalie, i responsabili UOR affinché possano essere elaborate e messe in campo le opportune azioni di miglioramento.

Obiettivo 6 – Avvio del sistema per la conservazione a norma dei documenti digitali contenuti nel sistema di Protocollo Informatico.

L'obiettivo è di avviare, così come da Decreto del Direttore Generale DG/2013/1071 del 24/07/2013, un processo teso alla realizzazione di un sistema di conservazione dei documenti informatici con la finalità di assicurare la conservazione, in modo permanente e con modalità digitali, dei documenti e dei fascicoli formati con strumenti informatici, tramite l'adozione di regole, procedure e tecnologie atte a garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati, in ottemperanza a quanto prescritto dalla normativa vigente in materia e dalle relative regole tecniche. A tal fine, nel predetto Decreto, il Direttore Generale ha nominato il "Responsabile della conservazione dei documenti informatici dell'Università degli Studi di Napoli Federico II" e ha delineato i compiti e l'ambito di responsabilità anche rispetto alle responsabilità del RSP e del CSI, in modo del tutto coerente rispetto al quadro nazionale normativo e regolamentare di riferimento.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

3. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate per le operazioni di formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici - anche in relazione alle norme sulla protezione dei dati personali - svolte con il sistema di protocollazione e gestione dei documenti.

3.1. Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

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

3.2. Generalità

Il RSP ha predisposto il piano di sicurezza, in collaborazione con il CSI, nel rispetto della normativa sulla protezione dei dati personali. Il Piano di sicurezza descritto nel presente Manuale riprende ed aggiorna quanto contenuto nell'ultima edizione Documento Programmatico sulla Sicurezza del 2011, approvato con Decreto Rettorale DR/2011/764 del 31.3.2011.

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.
Il RSP, in accordo con RSI (in particolare, con la Direzione tecnica elaborazione dati e microinformatica del CSI), ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

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

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati, solo in caso di necessità, dal titolare dei dati e, ove previsto, dalle forze dell'ordine.
Le politiche di sicurezza adottate ed i meccanismi di sicurezza implementati sono dettagliatamente descritti nell'**allegato 8**.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

3.3. Formazione informatica dei documenti – aspetti di sicurezza

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

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

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Tali documenti sono quindi materializzati su supporto cartaceo e quindi sottoscritti con firma autografa e sottoposti a registrazione e segnatura di protocollo, oppure sono gestiti in modalità digitale. In tal caso, i documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, PDF/A, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. A seguire, il responsabile appone la propria firma digitale (eventualmente apponendo una firma parallela se il documento risulta già firmato digitalmente da altro sottoscrittore), in modo tale da attribuire in modo certo la titolarità del documento informatico, la sua integrità e, se del caso, la riservatezza. Relativamente a tale aspetto, infatti, il titolare del certificato di firma può crittografare il documento, rendendone quindi decodificabile il contenuto solo da parte di predeterminati destinatari. In ogni caso, al fine di consentire l'accessibilità al documento amministrativo anche nel lungo termine, superati i limiti di validità di legge dei certificati digitali, non è consentita la registrazione nel PdP di documenti crittografati.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui agli artt. 37 e 51 del decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009 "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici" di seguito riportati:

Art. 37.
Riferimenti temporali opponibili ai terzi

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1. I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del codice.
2. I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 20, comma 3 del codice.
3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo.
4. Costituiscono inoltre validazione temporale:
a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272;
b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del codice;
d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14 , comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il decreto del Presidente della Repubblica 12 gennaio 2007, n. 18.

Art. 51.
Valore della firma digitale nel tempo

1. La firma digitale, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma digitale in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.

3.4. Gestione informatica dei documenti – aspetti di sicurezza

Il sistema operativo del PdP utilizzato dall'amministrazione/AOO, è – anche in base a quanto certificato dal Fornitore del PdP – conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi), in accordo con quanto prescritto dalla Circolare del 21 giugno 2001, n. AIPA/CR/31.

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- l'accesso al server del protocollo informatico esclusivamente agli utenti autorizzati;
- la memorizzazione dell'identificativo utente e della postazione di lavoro da cui sono svolte le attività più critiche e rilevanti ai fini della sicurezza svolte da ciascun utilizzatore del PdP, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette ed immodificabili.

Il sistema di gestione informatica dei documenti:

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

I suddetti obiettivi di sicurezza sono realizzati mediante l'attuazione di opportuni meccanismi di sicurezza di tipo informatico, organizzativo e infrastrutturale, corrispondenti alle funzioni di sicurezza definite nel Piano della Sicurezza del PdP. Tali meccanismi, adeguati a contrastare le minacce individuate, sono continuamente adeguate in funzione del progresso tecnologico e delle modifiche normative in materia di sicurezza ICT da parte del CSI, in accordo con RSP.

Maggiori dettagli sui componenti della sicurezza di tipo organizzativo, informatico ed infrastrutturale, alle modalità di trasmissione ed intercambio dati, alle funzioni di sicurezza per consentire l'accesso al PdP e ai documenti informatici in esso custoditi, nonché alle modalità di archiviazione dei dati sono riportati nell'allegato 8.

3.5. Politiche di sicurezza adottate dalla AOO

Le politiche ed i meccanismi di sicurezza riportati nell'allegato 8 stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

L'RSP si impegna, d'accordo con RSI, a procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza, da sottoporre all'approvazione e

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

all'autorizzazione da parte degli organi competenti prima di una loro effettiva adozione.

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti tra strutture interne all'Amministrazione e tra strutture dell'Ateneo e soggetti ed enti esterni.

Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo. Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

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

Il documento amministrativo, in termini tecnologici, è classificabile in

- informatico, quando – ai sensi dell'art. 1 comma 1 lettera p) del CAD – è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- analogico, quando – ai sensi dell'art. 1 comma 1 lettera p-bis) del CAD – è la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Quindi, nel seguito, si intende che un documento, anche se formato con strumenti informatici, è analogico se il suo contenuto viene rappresentato su supporto cartaceo e sottoposto quindi a firma autografa da parte del sottoscrittore.

Per evitare conflitti di notazione, il documento amministrativo informatico sottoscritto con firma digitale sarà denominato documento digitale.

Nei paragrafi seguenti verranno meglio approfondite le caratteristiche delle due tipologie di documenti.

4.1. Il documento informatico

Come già detto, il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. In particolare, i commi 1, 1-bis e 3 contenuti nell'art.20 del decreto legislativo del 7 marzo 2005, n.82, recante "Codice dell'Amministrazione digitale" prevedono che:

1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall' articolo 21.

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell' articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale [2]*.*

I commi 1 e 2 contenuti nell'art. 21 del CAD prevedono inoltre che:

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all' articolo 20, comma 3 , che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile . L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

Ai sensi degli artt. 23, 23-bis e 23-ter del CAD, inoltre, è prevista la possibilità di effettuare copie e duplicati di documenti informatici, in formato analogico o informatico. In particolare, il comma 5 dell'art. 23-ter (modificato dalla legge Crescita 2.0) prevede che*: "Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità".* Su tale previsione normativa si basa, come verrà più ampiamente detto nel prosieguo, la soluzione dell'Università per la produzione di copie conformi di documenti digitali registrati nel sistema del protocollo informatico.

[2] A tale riguardo, giova ricordare che, ai sensi dell'art. 37 comma 4 del DPCM 30.03.2009 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", il riferimento temporale contenuto nella segnatura di protocollo è una validazione temporale opponibile ai terzi.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

4.2. Il documento analogico - cartaceo

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

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

In generale, un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione a norma, quando disponibili e opportunamente regolamentate.

4.3. Formazione dei documenti – aspetti operativi

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

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

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

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

Le regole per la determinazione dei contenuti e della struttura dei documenti sono definite dai Responsabili delle singole UOR.

Il documento deve consentire l'identificazione dell'Amministrazione/UOR mittente, di norma, attraverso le seguenti informazioni:

- la denominazione e il logo dell'Amministrazione/UOR;
- l'indicazione completa dell'Amministrazione e dell'UOR/UU che ha prodotto il documento;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- l'indirizzo completo dell'Amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono della UOR/UU;
- il numero di fax della UOP.

Il documento deve inoltre recare almeno le seguenti informazioni:

- la data (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sottoscrizione autografa del responsabile del procedimento amministrativo (RPA) e/o del responsabile del provvedimento finale.

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'Amministrazione rende disponibili per via telematica, sul sito www.unina.it, moduli e *template* elettronici di carta intestata, validi a ogni effetto di legge.

4.4. Sottoscrizione di documenti informatici

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, ai sensi del Regolamento di Ateneo in materia di firma digitale, sono convertiti in pdf, uno dei formati standard previsti dalla normativa vigente in materia di archiviazione (pdf, pdf/A, tiff), al fine di garantirne l'immodificabilità. Il formato di firma previsto per i documenti amministrativi dell'Università è il Cades. L'estensione del file prodotto è in tal caso "p7m".

4.5. Apposizione della firma digitale

Per la sottoscrizione dei documenti informatici, quando prescritta, l'Amministrazione si avvale dei servizi di un'autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale.

Lo strumento che assicura il soddisfacimento dei requisiti di integrità, autenticità e non ripudio, in accordo con quanto prescritto dal Codice, è infatti la firma digitale, utilizzata quindi per sottoscrivere documenti informatici con valenza giuridico-probatoria.

I documenti possono essere sottoscritti da più soggetti: in tal caso, sono apposte firme multiple, di tipo parallelo o di tipo controfirma. La firma dell'intera busta crittografica è

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

prevista solo in casi particolari, espressamente previsti e regolamentati dallo specifico procedimento.

Nel caso di apposizione di firme multiple, i sottoscrittori successivi al primo devono effettuare preventivamente la verifica di validità ed integrità del documento che devono firmare.

4.6. Verifica delle firme con il PdP

I documenti sottoscritti con firma digitale sono sottoposti a verifica di validità e di integrità grazie all'utilizzo dei servizi di verifica disponibili in tutti i prodotti di mercato di firma digitale. Tale processo deve essere realizzato in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito dell'Agenzia per l'Italia digitale).

L'operazione di verifica deve essere svolta sia dal sottoscrittore che deve apporre una firma parallela (come detto nel paragrafo precedente), sia dal PdP in fase di registrazione del documento Anche nel PdP sono infatti previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare.

La sequenza delle operazioni previste nel PdP è la seguente.

- apertura della busta "virtuale" contenente il documento firmato, in formato p7m ("cades"), pdf ("pades") o xml ("xades");
- verifica della validità dei certificati di firma (sono più di uno nel caso di documento contenenti firme digitali multiple);
- verifica della integrità del documento;
- verifica che la firma del certificato di firma dell'utente sia apposta da una Certification Authority (CA) presente nell' elenco pubblico dei certificatori accreditati e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate con periodicità giornaliera,
- inserimento nel sistema documentale dell'Amministrazione sia del documento originale firmato sia del documento in chiaro,
- registrazione nei metadati di registrazione delle informazioni, immodificabili, relative all'esito delle verifiche di autenticità e integrità..

4.7. Requisiti degli strumenti informatici di scambio

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

- l'integrità del messaggio;
- la riservatezza del messaggio;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

Tali requisiti sono rispettati utilizzando in modo coordinato gli strumenti della PEC, della firma digitale e del Protocollo Informatico. Con particolare riguardo al PdP, l'interoperabilità avanzata di protocollo tra AOO, viene descritta più avanti nel presente Manuale.

Di seguito, si riportano le regole e le prassi utilizzate in Ateneo per l'invio e la ricezione di documenti (analogici o informatici e digitali), a seconda che la trasmissione sia formale o informale.

4.8. Documento ricevuto dalla AOO ("Entrata")

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

Un documento informatico può essere recapitato:
1. a mezzo posta elettronica convenzionale o certificata;
2. su supporto rimovibile quale, ad esempio, cd rom, dvd, floppy disk, tape, pen drive, etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

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

4.9. Documento inviato dalla AOO ("Uscita")

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

I documenti analogici sono spediti a mezzo posta convenzionale o corriere (interna nel caso di documenti spediti a destinatari interni all'Università), eventualmente via corriere o, a seconda dei casi, in modalità raccomandata con AR.

Nel caso di invio mediante raccomandata (PEC oppure postale), viene allegata alla registrazione di protocollo del documento la ricevuta di consegna: nel primo caso viene allegato il messaggio PEC contenente la ricevuta di consegna, nel secondo caso viene acquisita l'immagine della ricevuta cartacea di consegna.

4.10. Documento interno formale ("Tra Uffici")

Lo scambio tra UOR/UU di documenti informatici di rilevanza amministrativa giuridico-probatoria, avviene di norma attraverso il PdP, oppure per mezzo della posta elettronica convenzionale o, se è previsto l'invio anche del documento originale (nel caso di documenti analogici), mediante posta interna.

Più in dettaglio, se Il documento scambiato è informatico, esso viene prima sottoscritto con firma digitale e poi protocollato.

Se il documento è invece analogico, il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa e successivamente protocollato. Via PdP viene dunque resa disponibile al destinatario l'immagine del documento scansionato e l'originale viene custodito dal mittente, salvo i casi in cui, oltre all'inoltro informatico, il destinatario debba essere in possesso anche del documento originale. In tal caso, il documento viene prodotto (originale e minuta) con strumenti informatici e stampato. La firma autografa viene quindi apposta sia sull'originale che sulla minuta e, quindi, il documento viene protocollato: il mittente custodisce la minuta del documento. Il documento originale, interno, formale e analogico – completo di segnatura – viene quindi trasmesso, oltre che in forma elettronica via PdP, anche con i mezzi tradizionali all'interno dell'Amministrazione.

4.11. Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione. In alternativa al PdP, può essere utilizzata anche la posta elettronica (convenzionale oppure PEC).

4.12. Uso della posta elettronica certificata

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

L'utilizzo della posta elettronica certificata (PEC) consente di:

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

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

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

Inoltre, il Codice dell'Amministrazione digitale prevede che:

Articolo 47.

Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all' articolo 71;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO. Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo tra pubbliche amministrazioni.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

- redigere il documento con un sistema di videoscrittura;
- inserire nel campo indirizzo del documento i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del Ufficio Protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale (oppure PEC) del destinatario;
- allegare alla registrazione di protocollo la ricevuta dell'esito della trasmissione.

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

I messaggi di ritorno, che sono classificati in:

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

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

Tra i prossimi obiettivi dell'Ateneo (Obiettivo 5 del cronoprogramma riportato in allegato 7), RSP provvederà a organizzare con l'Amministrazione e con l'UOP dell'Amministrazione Centrale l'avvio del modulo di interoperabilità avanzata presente nel PdP (nella versione compatibile con la Circolare AIPA del 7 maggio 2001, n. 28), anche alla luce dell'imminente emanazione della Circolare dell'Agenzia per l'Italia Digitale del 23 gennaio 2013, n. 60 in materia di segnatura di protocollo. Il modulo informatico presente nel PdP dovrà quindi essere opportunamente configurato in modo tale da adeguarlo al flusso informativo di trattamento della posta in arrivo descritto nel prossimo capitolo. In parallelo, dovrà essere opportunamente addestrato il personale incaricato del trattamento all'utilizzo della nuova funzionalità.

Attualmente, nelle more dell'avvio della gestione dell'interoperabilità avanzata con altre PPAA, l'Amministrazione comunque utilizza la PEC come strumento per trasmettere documenti informatici a altre AOO oppure a cittadini o soggetti esterni all'Ateneo. Nel caso di invio, il documento allegato al messaggio PEC è l'immagine del documento scansionato e dotato di segnatura di protocollo, oppure, il documento

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

digitale insieme alla copia dello stesso completa di timbro crittografico contenente i dati di registrazione, oppure la copia conforme automatizzata del documento stesso (in formato pdf, completo del contrassegno prodotto in automatico dal sistema PdP). In ogni caso, come detto anche più avanti, alla registrazione di protocollo viene allegata la ricevuta di consegna. Nel caso di ricezione da altre AOO, da cittadini, imprese o professionisti, vengono registrati nel PdP, se presenti, da parte della UOR ricevente: il documento informatico primario allegato al messaggio di posta e i relativi allegati. In aggiunta, se rilevante ai fini del procedimento amministrativo, viene registrato come ulteriore allegato della registrazione anche il messaggio PEC (in formato "eml").

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

5.1. Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno dell'Amministrazione, si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.
Essi si riferiscono ai documenti:

- ricevuti dall'Amministrazione, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno all'Amministrazione stessa. Tali documenti sono individuati, rispettivamente, come in "Entrata", oppure "Tra Uffici";
- inviati dall'Amministrazione, all'esterno o anche all'interno in modo formale. Tali documenti sono individuati, rispettivamente, come in "Uscita", oppure "Tra Uffici".

I flussi gestiti all'interno del sistema archivistico dell'Amministrazione dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.

Come previsto dalla normativa vigente, i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima. I flussi relativi alla gestione dei documenti all'interno dell'Amministrazione sono descritti graficamente nel paragrafo seguente prendendo in esame quelli che possono avere rilevanza giuridico probatoria.

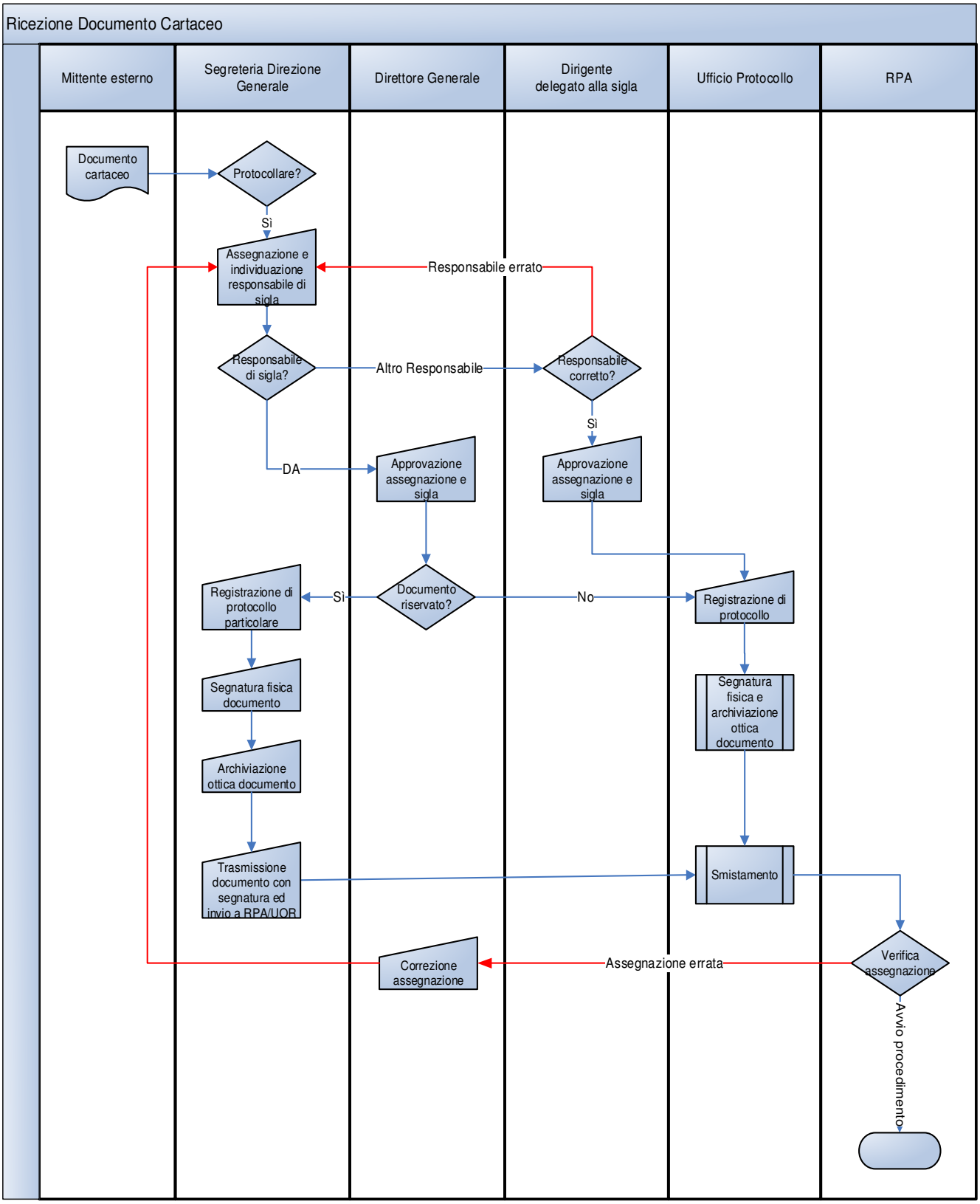
5.2. Flusso dei documenti ricevuti

I documenti, analogici oppure informatici, in ingresso ad una data UOR dell'Amministrazione possono essere di tipo "Entrata" se ricevuti da un soggetto esterno all'AOO (altra PA, cittadino, società esterna, professionista, dipendente) oppure possono essere originati da altra UOR (in tal caso sono definiti "Tra Uffici"). In ogni caso, i documenti ricevuti da una UOR possono essere trattati, per competenza, all'interno della UOR stessa, oppure smistati per posta interna alla UOR di competenza.

5.2.1. Flusso documenti cartacei "Entrata"

Di seguito, si riporta lo schema del flusso della corrispondenza in ingresso, di tipo analogico:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



Tale diagramma di flusso rappresenta, per l'Amministrazione Centrale, il ciclo di vita in entrata che, più dettagliatamente, si articola nelle seguenti fasi:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Accettazione (fase non riportata nel diagramma): in questa fase l'UOP-Servizio smistamento posta della UOR riceve il documento proveniente da un mittente esterno all'Amministrazione (altro ente, privato cittadino etc.). Nel caso sul plico sia riportata la dicitura "offerta", "gara d'appalto" o simili, il plico viene inviato all'UOP per la registrazione di protocollo e quindi, da questi al Responsabile del procedimento;

- Smistamento: nel caso in cui il plico o il suo contenuto siano indirizzati ad altra UOR, viene effettuata uno smistamento alla UOR destinataria per posta interna;

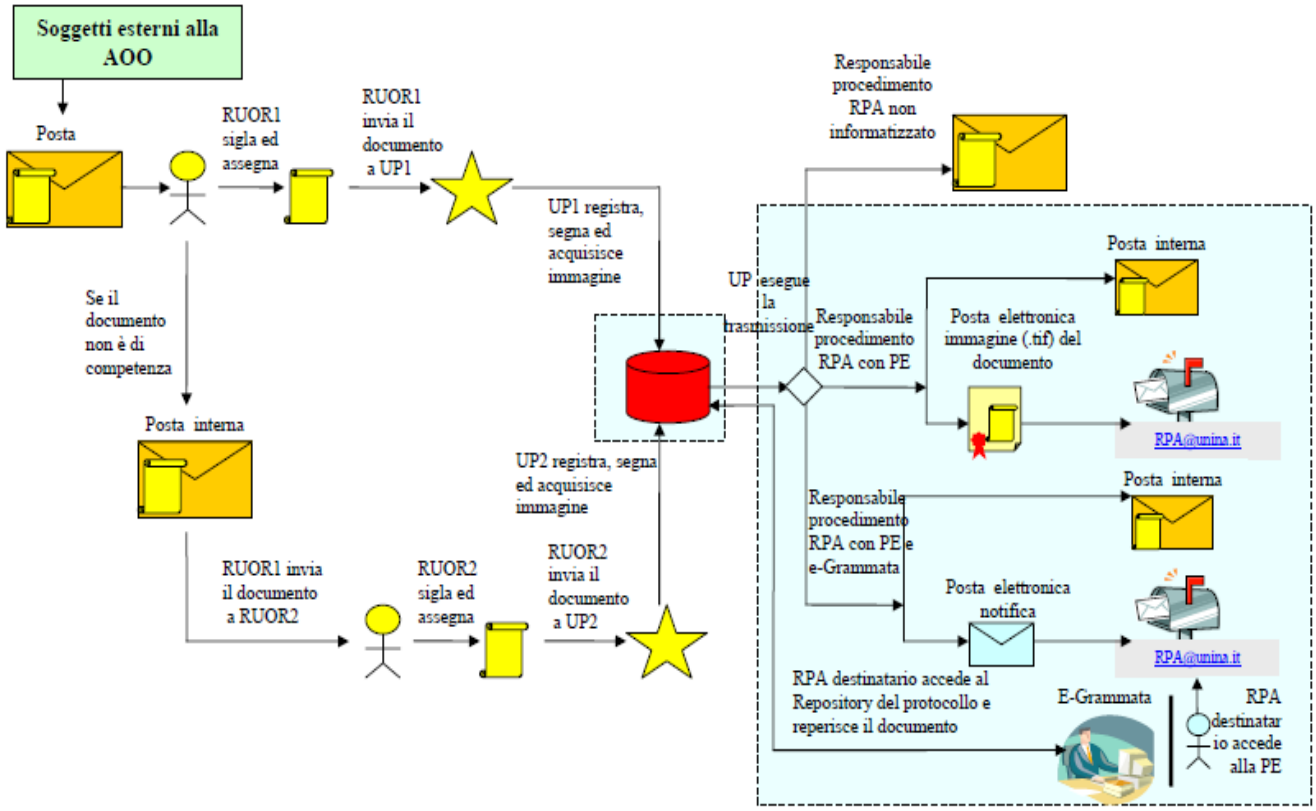
- Assegnazione: il documento viene inviato al Responsabile UOR (nel caso dell'Amministrazione Centrale, alla Segreteria del Direttore Generale) che stabilisce se il documento è da inviare per competenza al dirigente delegato alla sigla, oppure no. Nel primo caso, la Segreteria invia il documento al delegato. Il responsabile preposto alla sigla (Direttore Generale o Responsabile UOR o Delegato alla sigla) provvede ad identificare l'ufficio destinatario del documento al quale è assegnata la responsabilità del procedimento amministrativo (RPA) e gli eventuali ulteriori assegnatari;

- Protocollazione e Classificazione: in questa fase l'UOP mediante le funzioni del PdP provvede a:
    - attribuire un numero e una data di protocollo al documento
    - apporre la segnatura al documento cartaceo e, contestualmente, effettuare l'acquisizione dell'immagine del documento completa di segnatura
    - aggiungere nell'archivio del PdP l'immagine del documento e i dati di registrazione di cui si forniranno maggiori dettagli nel prosieguo del presente documento
    - inserire tutti gli assegnatari come destinatari di copia o di copia conoscenza del documento, mantenendo l'ordine apposto sul documento dal Responsabile

- Smistamento: l'originale cartaceo è inoltrato al primo assegnatario, insieme al rapporto di consegna. Tutti i restanti assegnatari (compreso il primo), se si tratta di UU dell'Amministrazione, dispongono dell'immagine scansionata del documento originale. Nel caso in cui il destinatario non sia utente del PdP, viene inoltrata all'interessato da parte dell'UOP di afferenza un messaggio di posta elettronica con allegata l'immagine del documento, oppure, a seconda del tipo di procedimento, una copia cartacea consegnata a mano mediante posta interna.

Nella figura seguente viene evidenziato il flusso informativo a valle della registrazione di protocollo, qualora RPA non disponga di una posizione nell'organigramma del Protocollo, ragion per cui deve essere destinatario (se non è primo assegnatario) di comunicazione via e-mail, oppure, via PEC.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



Legenda Acronimi:

UOR	= Unità Organizzativa Responsabile
RUOR	= Responsabile UOR
UP	= Ufficio Protocollo
RPA	= Responsabile Procedimento Amministrativo
AOO	= Area Organizzativa Omogenea
PE	= Posta Elettronica
PEC	= Posta Elettronica Certificata

Legenda simboli:

= Utente

= Utente del sistema di protocollo E-Grammata

= Ufficio di Protocollo della UOR (dotato del sistema E-Grammata)

= Sistema Informatico di Protocollo E-Grammata e repository documentale

= Posta Ordinaria (o interna)

= Messaggio di Posta Elettronica

= Messaggio PEC di sola notifica

= Documento informatico con firma digitale

= Riproduzione informatica (.pdf) del Documento informatico con sovraimpressione della segnatura di protocollo

= Documento Cartaceo

= Riproduzione cartacea del Documento informatico con evidenza a stampa della segnatura di protocollo

= Casella di Posta Elettronica (Certificata o non)

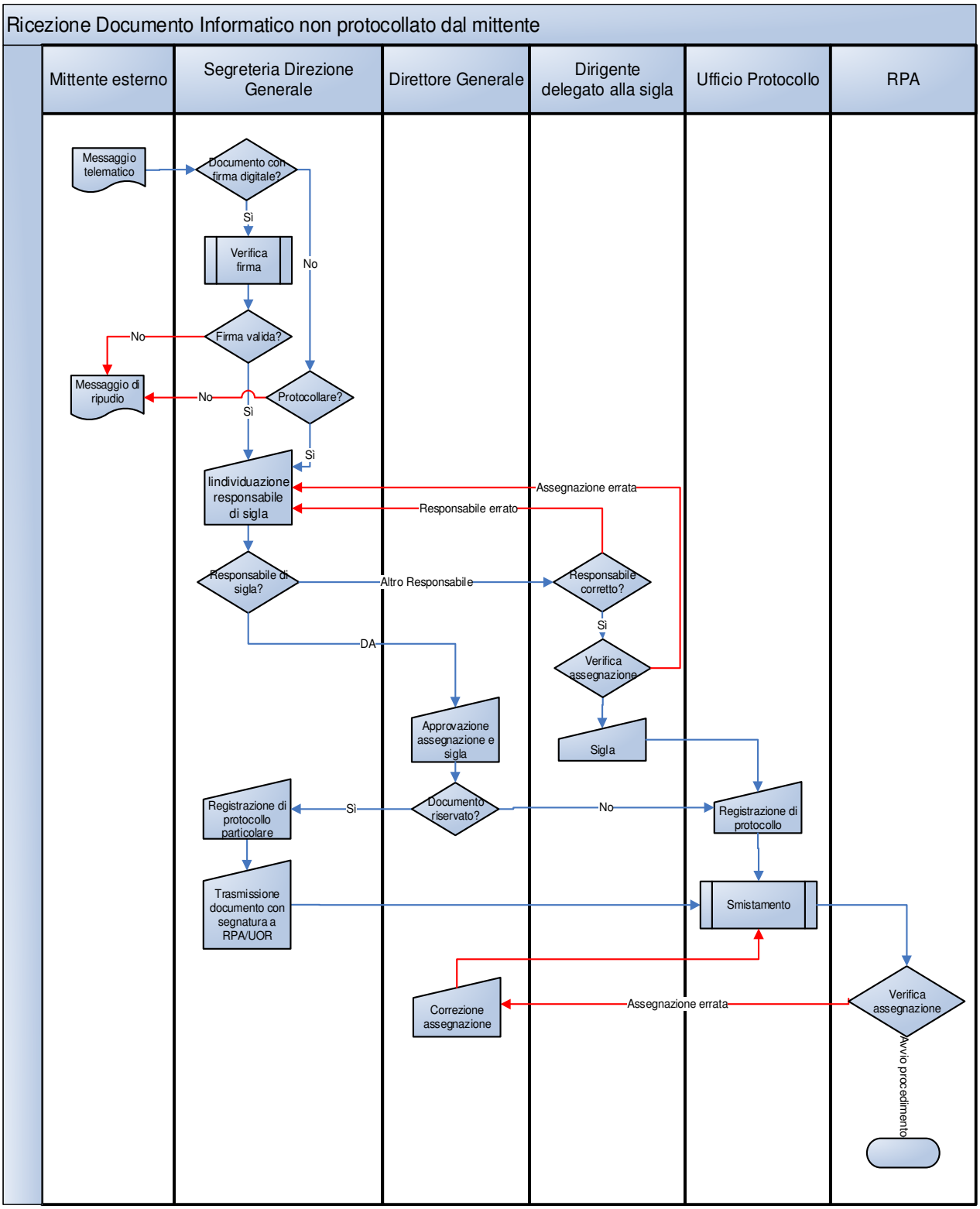
= Messaggio PEC con files allegati interoperabilità (.p7m e .xml)

= Immagine (.tif) del documento cartaceo segnato ed acquisito con scanner

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

5.2.2. Flusso documenti informatici in "Entrata"

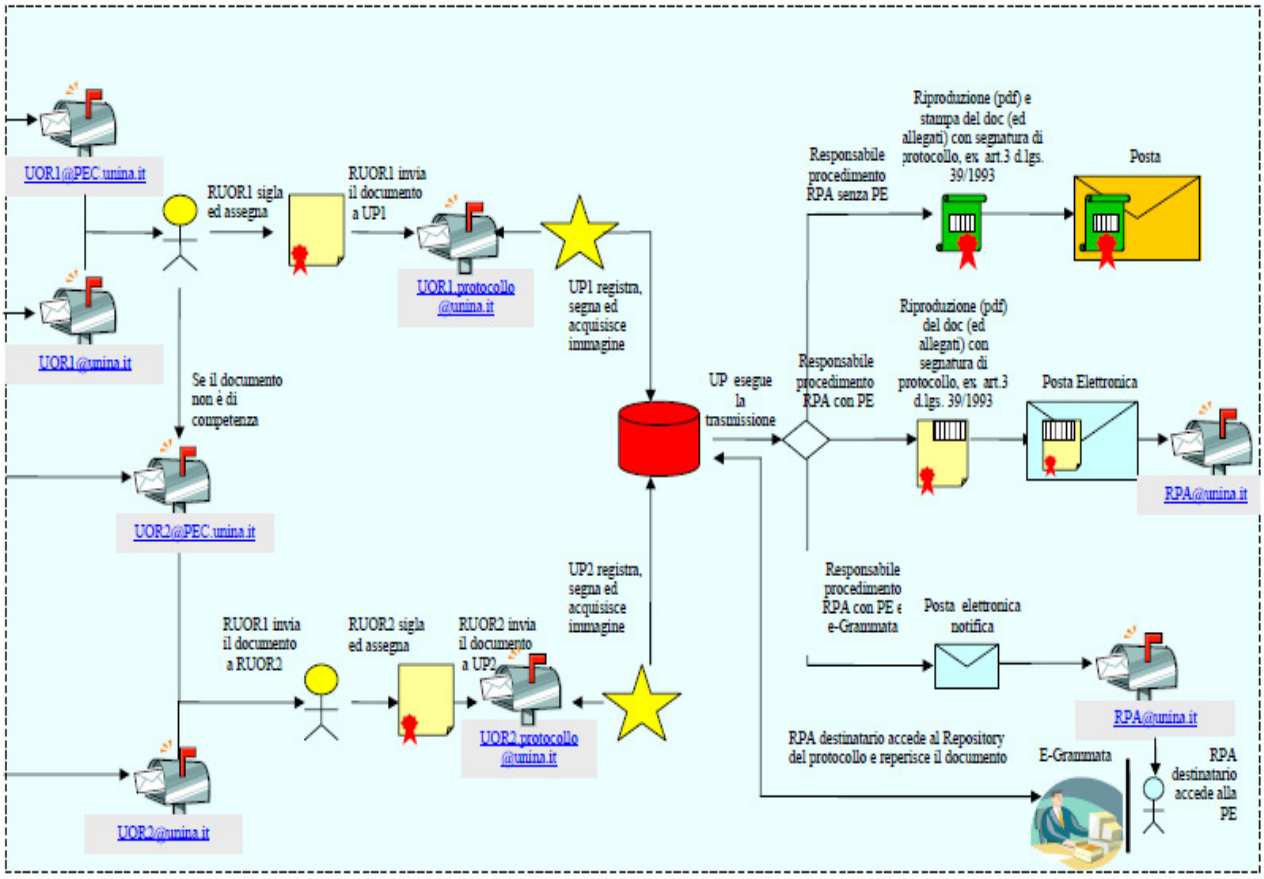
Di seguito, il diagramma di flusso del processo di assegnazione, sigla e protocollazione dei documenti informatici in arrivo dall'esterno della AOO.



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

I documenti informatici possono essere recapitati alla UOR (e quindi, alla AOO nel suo complesso) via posta elettronica, oppure PEC, oppure mediante consegna di unità magneto-ottiche (dvd/ CD-Rom, etc.).

Nel diagramma che segue, sono rappresentate tutte le fasi (fino alla consegna a RPA) nei primi due casi:



Lo schema sopra riportato si riferisce al caso di documenti in ingresso alla AOO, di tipo informatico, in generale quindi ricevuti via posta elettronica (certificata e non), all'indirizzo della UOR.

L'Amministrazione Centrale, oltre a gestire i propri indirizzi di posta elettronica (diramm@unina.it) e PEC (diramm@pec.unina.it) di servizio, gestisce anche i corrispondenti indirizzi istituzionali dell'intera AOO: ateneo@unina.it e ateneo@pec.unina.it.

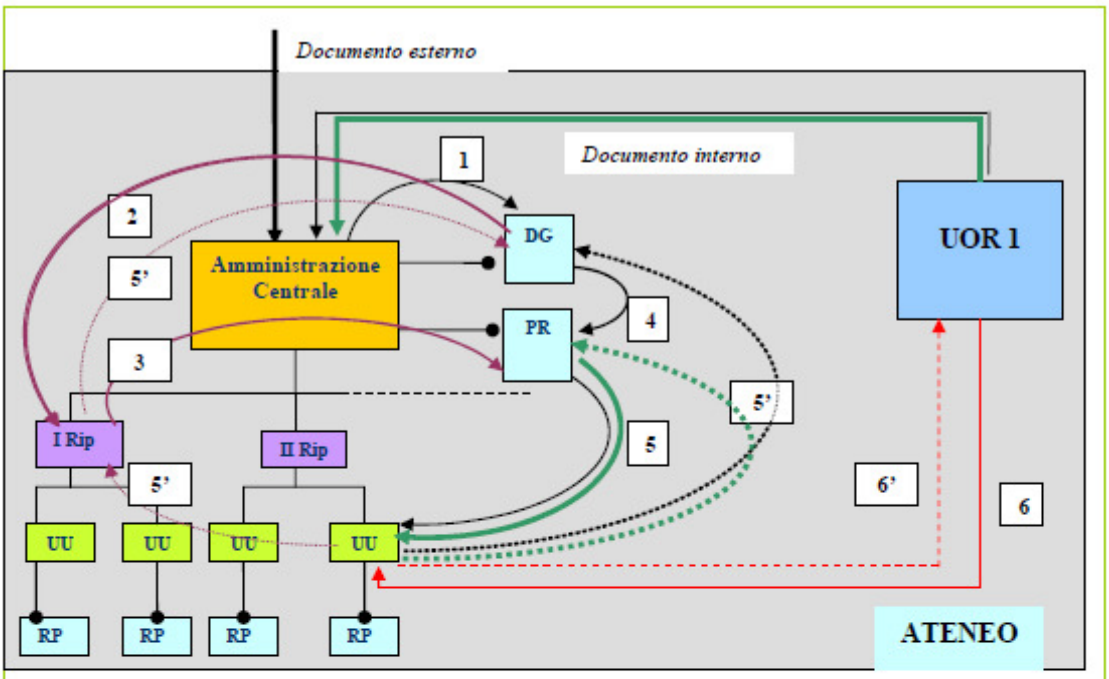
5.2.3. Flusso di documenti interni formali ("Tra Uffici")

Per sorgente interna dei documenti si intende qualunque RPA che invia formalmente, per il tramite dell'UOP della propria UOR, la propria corrispondenza ad una distinta UOR dell'Amministrazione per essere a sua volta nuovamente trasmessa, nelle forme opportune, ad altro UOR o UU della stessa Amministrazione.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

In generale, tali documenti devono recare la firma del Responsabile UOR e la trasmissione può avvenire solo tra UOR. Se lo scambio di documenti avviene intra-UOR, il documento può essere sottoscritto anche dal Responsabile UU. Nel caso in cui un RPA non responsabile di struttura debba inviare un documento via PdP, RPA si configura come mittente esterno e può rivolgersi al UOP della propria struttura per la registrazione di protocollo che, in tal caso, è "In entrata". In alternativa, RPA può inviare il documento alla UOR destinataria che provvederà a protocollarlo per il tramite del proprio UOP.

Lo schema seguente è relativo allo scambio di documenti interni formali tra due UOR: l'Amministrazione Centrale e un'altra UOR (Dipartimento, Centro, etc.):



1 = Consegna della posta (doc cartacei) alla Direzione Amministrativa che sigla ed assegna.

2 = Trasmissione del documento cartaceo a Resp. Sigla di II livello (Dirigente Ripartizione) che sigla ed assegna

3 = Trasmissione del documento cartaceo all'Ufficio di Protocollo che ne gestisce la spedizione agli assegnatari e la gestione del flusso elettronico.

4 = La Direzione Amm.va (oppure il Responsabile di Sigla) trasmette il documento cartaceo all'Ufficio Protocollo.

5 = L'Ufficio Protocollo registra (se documento esterno o comunque sprovvisto di codice PG) e smista cartaceo ed elettronico a tutti gli assegnatari.

5' = Restituzione del documento cartaceo al Responsabile di Sigla per cambio assegnatario

6 =Invio del documento (flusso cartaceo ed elettronico) da parte dell'UOR mittente direttamente all'Ufficio.

6' = L-Ufficio restituisce il documento (sia elettronico che cartaceo) nel caso di errato invio.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Il documento interno scambiato tra UOR e UU dell'Ateneo è di tipo informatico secondo i formati standard illustrati nel precedente capitolo. In generale, il documento da trasmettere tramite PdP potrà quindi essere un'immagine scansionata di un documento cartaceo, oppure un documento firmato digitalmente, oppure un messaggio PEC ricevuto dall'esterno e acquisito al PdP. Infatti, nel caso dei documenti cartacei, ciascun documento è redatto in unico esemplare con firma autografa del responsabile UOR e, a valle della registrazione ed acquisizione nel sistema di PdP, è conservato dalla struttura mittente nel fascicolo relativo all'affare o al procedimento amministrativo trattato.

In ogni caso, sia che il documento originale sia cartaceo, sia che il documento originale sia digitale, ciascuna struttura, attraverso il personale appositamente incaricato, è tenuta a consultare con frequenza giornaliera la propria lista di lavoro disponibile sul sistema di PdP e di provvedere quindi alla presa in carico delle comunicazioni di propria competenza oppure, se non di propria competenza, alla loro restituzione al mittente.

Tuttavia, in deroga a quanto precedentemente espresso, alcuni documenti finalizzati alla trasmissione di atti originali analogici allegati continuano ad essere inviati, oltre che elettronicamente, anche in formato cartaceo, ad esempio: le istanze ed i certificati degli interessati per ottenere benefici normativi (es: 150 ore, etc.), le istanze ed i certificati di giustificazione delle assenze dal servizio, le dichiarazioni dei responsabili delle strutture per il pagamento delle indennità accessorie, i documenti contabili per la loro liquidazione, i registri delle attività didattiche, i verbali degli esami di profitto, i verbali dei dipartimenti, le istanze di partecipazione a procedure di valutazione comparativa del personale, i modelli con le nomine degli incaricati al trattamento dei dati personali, etc.). In tal caso, il documento è prodotto in originale e minuta ed inoltre, in fase di registrazione di protocollo, viene segnalato nel campo "Note di registrazione" - disponibile nel Protocollo Informatico - che il documento (con gli atti allegati) è inviato anche in forma cartacea.

Inoltre, in deroga alla regola generale che lo scambio di documenti possa avvenire solo tra UOR e non tra UOR e UU ad esse afferenti, presso l'Amministrazione Centrale è in uso **l'iter semplificato di presa in carico** dei documenti da parte degli uffici dell'Amministrazione Centrale, qualora i documenti si riferiscano a procedimenti di ordinaria amministrazione. Non appare superfluo rammentare che in tal caso, ciascuna struttura mittente trasmette elettronicamente i documenti via PdP (e, nei casi richiamati in precedenza, anche in formato cartaceo) indirizzandoli direttamente ed esclusivamente all'ufficio competente che prende in carico tali documenti senza dover necessariamente attendere formale ed esplicita assegnazione da parte del proprio responsabile.

L'elenco completo ed aggiornato dei procedimenti amministrativi che devono essere sottoposti all'iter semplificato di presa in carico è reperibile nella sezione "Protocollo" sul sito dedicato all'eGovernment dell'Ateneo, all'indirizzo http://www.praxis.unina.it,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

con l'indicazione dell'ufficio dell'Amministrazione Centrale competente e dunque, sulla base di quanto precedentemente detto, destinatario unico e diretto della registrazione di protocollo del documento.

Per quanto riguarda i documenti relativi a procedimenti non compresi nell'elenco dei procedimenti sottoposti all'iter semplificato di presa in carico, il flusso operativo prevede l'assegnazione da parte del Direttore Generale o di un responsabile di ripartizione. In tal caso, la struttura mittente protocolla e invia (elettronicamente o, salvo i casi su esposti, anche in modalità cartacea) la pratica direttamente alla Amministrazione Centrale che avvierà quindi la detta procedura di assegnazione e smistamento del documento all'ufficio competente illustrata nel successivo capitolo 6.

5.2.4. Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla Segreteria di Direzione Generale. Tale casella è consultata almeno con frequenza giornaliera, fermo restando che un meccanismo di notifica invia un alert sulla data casella di posta elettronica convenzionale della Segreteria.

Quando i documenti informatici pervengono a tale unità organizzativa, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento procede a salvare l'intero messaggio in formato "eml", completo dei dati di trasporto (firmati elettronicamente dal Gestore) e di quelli relativi al messaggio vero e proprio, completo degli eventuali allegati. I documenti allegati al messaggio di posta (tra cui il file primario stesso), insieme all'itero messaggio salvato, vengono quindi inviati via posta elettronica all'UOP con i metadati minimi di registrazione, inclusi i destinatari della registrazione. Il destinatario di protocollo può essere un ufficio dell'Amministrazione Centrale o altra UOR dell'Ateneo.

L'addetto del Protocollo Generale controlla quotidianamente i messaggi pervenuti nella casella di posta convenzionale e verifica se ci sono messaggi da protocollare.

Nel caso di invio su posta convenzionale, il flusso operativo descritto è uguale a quello descritto per la PEC, con l'unica differenza che il messaggio è trattato alla stregua di una comunicazione cartacea: il suo contenuto è stampato, assegnato e, quindi, inviato all'Ufficio Protocollo per la registrazione nel PdP.

5.2.5. Ricezione di documenti informatici sulla casella di posta elettronica certificata non istituzionale

Il flusso operativo appena descritto è utilizzato anche dalle Ripartizioni dell'Amministrazione Centrale e dai Dipartimenti (il cui indirizzo PEC è pubblicato in

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

IPA) oppure dalle restanti UOR dotate anch'esse di casella PEC. In quest'ultimo caso, la registrazione di protocollo è effettuata dalla UOR stessa.

5.2.6. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.
Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, l'Amministrazione si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

5.2.7. Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta o ritirati dal personale dell'Amministrazione dagli uffici postali sono consegnati alla UOP servizio smistamento e da questo alla Segreteria della Direzione Generale oppure, nel caso di UOR diverse dalla Amministrazione Centrale, al responsabile della UOR per lo svolgimento del processo di sigla e di assegnazione della pratica.
Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti. Nel caso l'indirizzo riportato sulla busta sia quello di una diversa UOR, il plico viene smistato in giornata per posta interna alla UOR destinataria.

5.2.8. Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali

Poiché l'Amministrazione è organizzata per ricevere documenti su carta attraverso qualsiasi UOR/UU aperta al pubblico, oltre, ovviamente attraverso il Protocollo Generale, il personale preposto all'apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.

5.2.9. Errata ricezione di documenti digitali

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

5.2.10. Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente alla UOP dell'Amministrazione documenti indirizzati ad altri soggetti. Possono verificarsi le seguenti possibilità:

- busta indirizzata ad altra UOR della stessa Amministrazione:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

a) se per errore la corrispondenza viene recapitata ad una UOR non destinataria del plico, quest'ultima, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti ma rilascia ricevuta al mittente e invia, nella stessa giornata, prima della chiusura del protocollo, la posta alla UOR interessata il plico, affinché possa essere sottoposto al processo di apertura, sigla ed assegnazione da parte del Responsabile della UOR o dal Responsabile di Sigla, se designato;
b) se la busta viene aperta per errore, il documento è protocollato in entrata inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore", si pone come destinataria la UOR responsabile del procedimento destinataria e si invia alla UOR stessa il plico, apponendo sulla busta la dicitura "Pervenuta ed aperta per errore";

- busta indirizzata ad altra amministrazione:

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

5.2.11. Attività di protocollazione dei documenti

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e "segnati" nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliate nel capitolo 10. Ogni UOR è autorizzata dall'amministrazione, per il tramite dei propri UOP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in entrata.

5.2.12. Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti informatici comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica.
Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'Amministrazione con gli standard specifici.

Nel caso di ricezione di messaggi di protocollo interoperabili da parte di altra amministrazione pubblica, come già detto in precedenza, il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- messaggio di conferma di protocollazione: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- messaggio di notifica di eccezione: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
- messaggio di aggiornamento di protocollazione: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

Attualmente, vista lo scarso numero di AOO interoperabili, non si è ritenuto utile attivare tale modalità di inoltro ricevute nel caso di ricezione di documenti informatici interoperabili. Come già detto in precedenza, nelle more dell'attivazione del modulo di interoperabilità avanzata del PdP, il messaggio PEC viene protocollato in formato "eml", completo cioè di tutti i dati di certificazione, oltre che del corpo del messaggio e degli allegati eventualmente presenti.

5.2.13. Rilascio di ricevute attestanti la ricezione di documenti cartacei

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

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata a una UOP di protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, la UOP che lo riceve è autorizzata a rilasciare ricevuta con gli estremi della segnatura, se contestualmente alla ricezione avviene anche la protocollazione. Tale operazione è svolta mediante un'apposita funzionalità del PdP che consente di produrre una ricevuta di avvenuta protocollazione, in cui sono riportate la data di consegna, la data e l'ora di registrazione di protocollo, la posizione organizzativa dell'ufficio mittente e la sigla dell'operatore.

5.2.14. Archiviazione dei documenti informatici

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.
I documenti ricevuti per via telematica sono resi disponibili alle UOR e agli UU destinatari, attraverso la rete interna dell'Amministrazione, subito dopo l'operazione di smistamento e di assegnazione.

5.2.15. Archiviazione delle rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, possono essere acquisiti in formato immagine attraverso un processo di scansione.
Il processo di scansione avviene in diverse fasi:

- apposizione sul documento dell'etichetta contenente la segnatura di protocollo;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

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

I documenti cartacei dopo l'operazione di riproduzione in formato immagine e di registrazione di protocollo sono disponibili a UOR/UU/RPA destinatari per i successivi adempimenti amministrativi. Nel caso in cui il destinatario non sia utente del PdP, la copia cartacea del documento viene inviata da UOP via posta all'indirizzo istituzionale dell'interessato.

I documenti con più destinatari, sono riprodotti in formato immagine ed inviati solo in formato elettronico. Il documento cartaceo originale viene inviato al primo destinatario.

5.2.16. Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla UOP eseguono la registrazione del documento in base alle informazioni relative all'assegnazione riportate sul documento (o, nel caso di documento informatico, nel messaggio di posta elettronica che riporta in allegato il documento da protocollare), alla classificazione del documento e procede quindi allo smistamento alla UOR/UU/RPA. Nel caso di assegnazione ad UOR, questa:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, ritrasmette il documento alla UOP di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA.

5.2.17. Conservazione dei documenti nell'archivio corrente

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

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

Tali operazioni sono svolte in fase di registrazione di protocollo dall'UOP di competenza sulla base delle indicazioni fornite dal responsabile di sigla, ferma

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

restando la possibilità per ciascun destinatario di modificare i dati di classificazione e fascicolazione della propria copia del documento.

5.2.18. Conservazione dei documenti e dei fascicoli nella fase corrente

All'interno di ciascun ufficio utente di ciascun UOR dell'Amministrazione sono stati individuati e formalmente incaricati gli addetti alla organizzazione e tenuta dei fascicoli "attivi" (e chiusi in attesa di versamento nell'archivio di deposito) e alla conservazione dei documenti al loro interno. Generalmente i responsabili della organizzazione e tenuta dei documenti e dei fascicoli nella fase corrente sono gli stessi RPA.

5.3. Flusso documenti inviati dalla AOO

Si definisce protocollazione in uscita la registrazione di un documento e dei suoi allegati il cui destinatario sia un soggetto (persona fisica o giuridica) esterno all'Università degli Studi di Napoli Federico II. Sono definiti come soggetti esterni anche i dipendenti, qualora il documento da inviare, pur contenendo nell'indirizzo l'indicazione della UOR/UO di afferenza del dipendente, sia da considerarsi "ad personam".

Un documento in uscita dalla UOR potrà, in generale, essere destinato:

a) ad un ente o ad un soggetto esterno all'Ateneo;
b) ad un dipendente dell'Ateneo;

oppure,

c) ad una struttura dell'Ateneo (provvista o meno di protocollo informatico).

Il caso c) è relativo ad una protocollazione interna ed diffusamente trattato nel relativo paragrafo.

E' bene notare che se la comunicazione (indirizzata ad un dipendente presso la struttura di appartenenza) è di carattere personale, ragion per cui il destinatario non è la struttura, bensì è il dipendente stesso selezionato dalla anagrafica, il documento non sarà visualizzato dalla struttura di afferenza del dipendente. Tale modalità è sconsigliabile, a meno di casi specifici, in quanto interrompe il flusso documentale e rende non fruibile il documento elettronico da parte del destinatario. In generale, se il documento è indirizzato al soggetto che ricopre la carica istituzionale della struttura (ad esempio: Al prof. XXXXXX – Direttore del Dipartimento YYYYY), UOP deve indirizzare il documento alla sola struttura indicata.

Il ciclo di vita in uscita (verso altre AOO) si articola (per i documenti analogici) nelle seguenti fasi:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Composizione e Classificazione: l'ufficio mittente provvede alla redazione del documento e della minuta di accompagnamento e all'attribuzione del codice di titolazione. L'RPA appone la propria sigla sulla minuta e sul documento;

- Approvazione: il documento viene sottoposto all'approvazione da parte del responsabile UOR. L'approvazione avviene mediante l'apposizione delle firme autografe sulla minuta e sul documento. Per l'Amministrazione Centrale, se il documento è relativo ad un procedimento che prevede l'apposizione della firma del Direttore Generale, il documento stesso viene sottoposto alla firma del Direttore. Il documento viene quindi consegnato all'UOP;

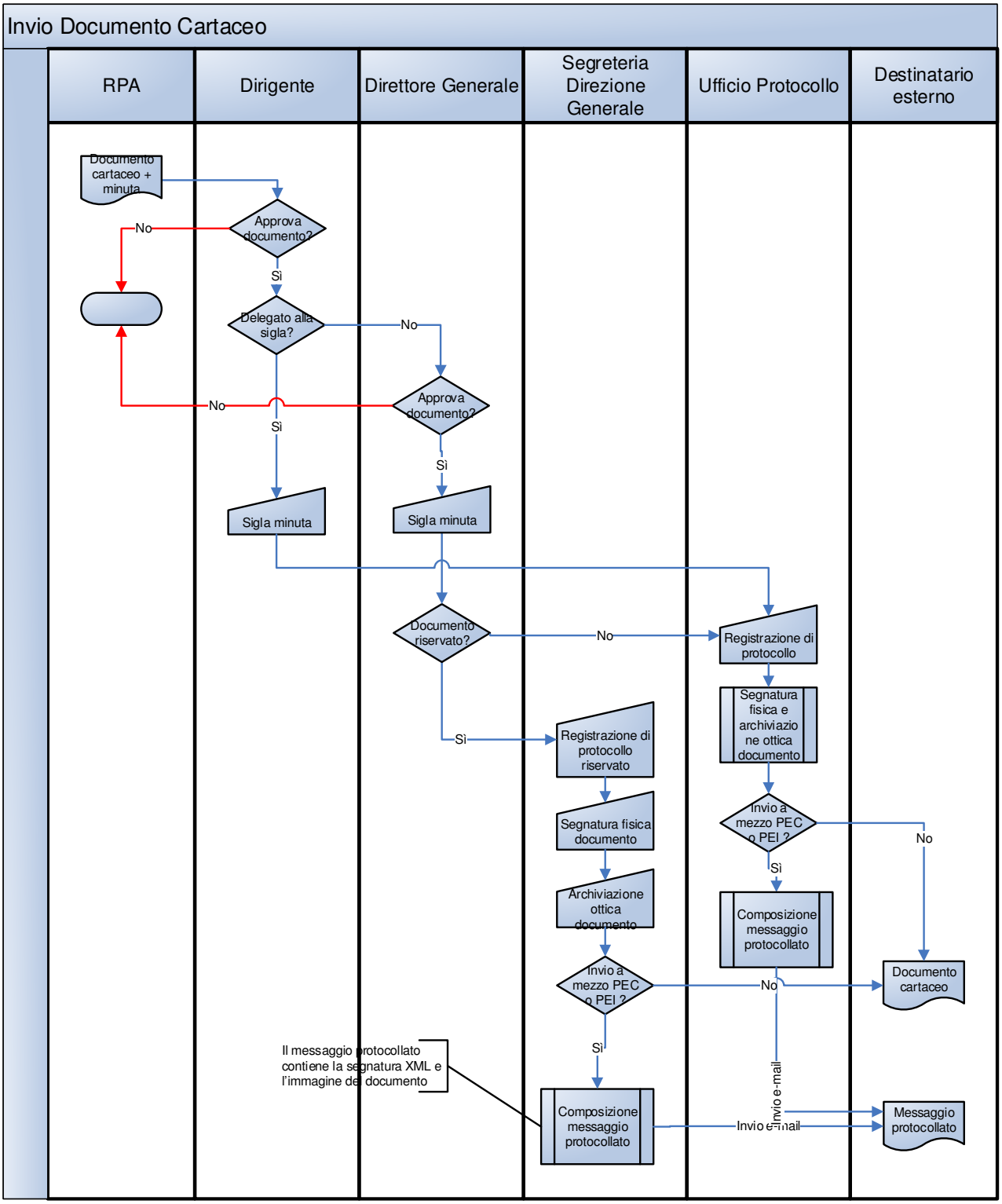
- Protocollazione: in questa fase, UOP provvede a:
  - attribuire un numero e una data di protocollo al documento
  - apporre la segnatura al documento cartaceo e alla minuta e contestualmente a effettuarne la conversione ottica
  - inserire nell'archivio del sistema di Protocollo l'immagine del documento e i dati di registrazione.

- Invio: il documento viene spedito. La minuta di accompagnamento torna all'ufficio mittente.

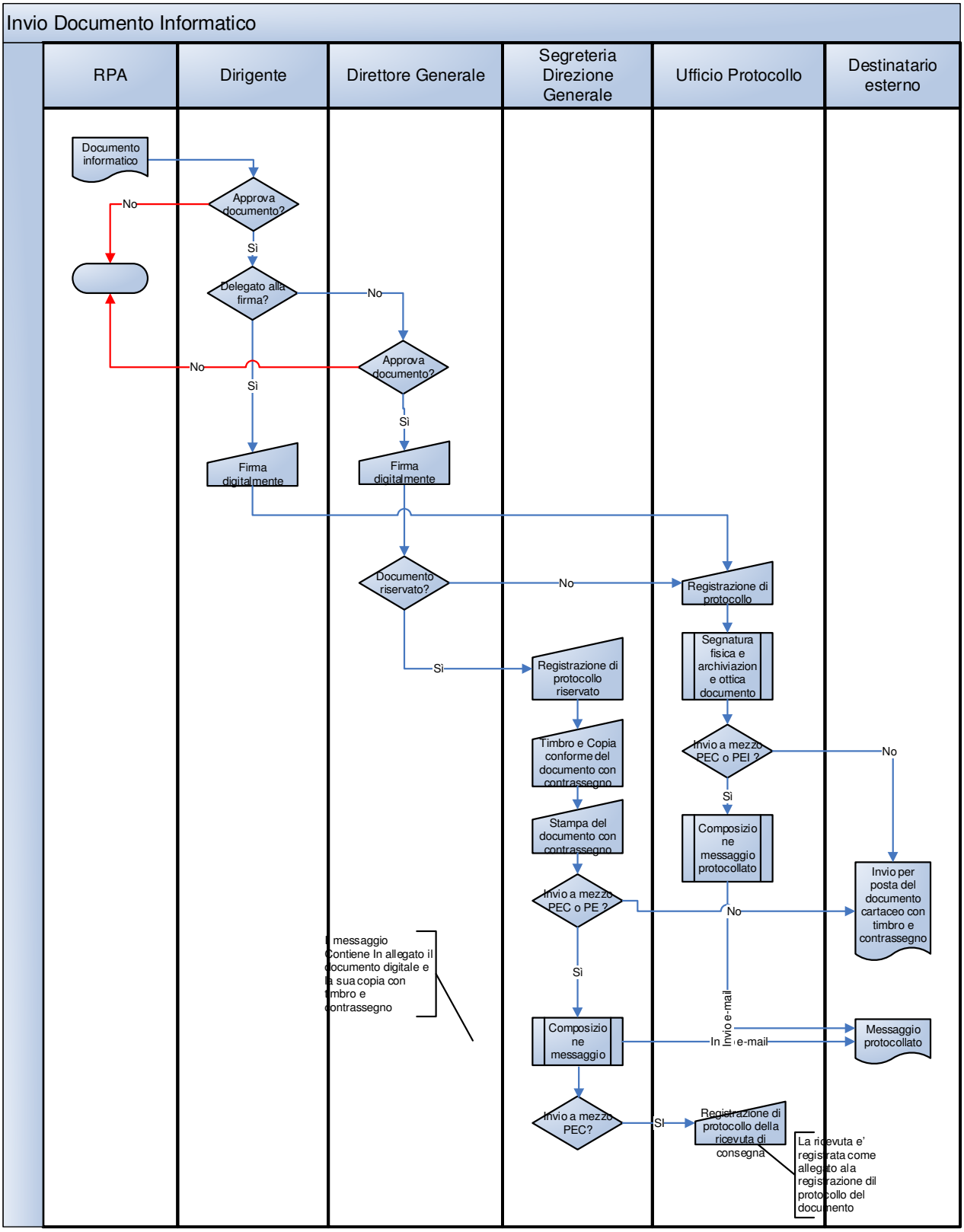
Nel caso in cui il documento sia spedito mediante raccomandata AR, viene acquisita l'immagine della ricevuta di ritorno ed allegata alla registrazione di protocollo del documento a cui si riferisce da parte dell'UOP della UOR interessata.

Di seguito, sono dettagliate le fasi del flusso operativo sopra schematizzato nel caso di invio di documenti analogici e, quindi, a seguire, nel caso di invio di documenti informatici.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

5.3.1. Sorgente interna dei documenti

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'Amministrazione nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra Amministrazione. Una struttura dell'AOO può comunque inviare documenti ad altro ufficio (UU o UOR) della stessa Amministrazione. L'unità organizzativa mittente all'AOO che invia la corrispondenza svolge quindi il ruolo di "sorgente interna dei documenti". Il flusso di lavoro è stato ampiamente descritto nel precedente paragrafo 5.2.3, relativamente al flusso "tra uffici".

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

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

5.3.2. Verifica formale dei documenti

Ogni UOR è autorizzata dall'amministrazione, per il tramite dei propri UOP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita. Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR, attraverso i propri UOP. Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

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

5.3.3. Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata dai singoli RPA/UU/UOR, attraverso i propri UOP abilitati in quanto collegati al sistema di protocollo informatico dell'amministrazione.

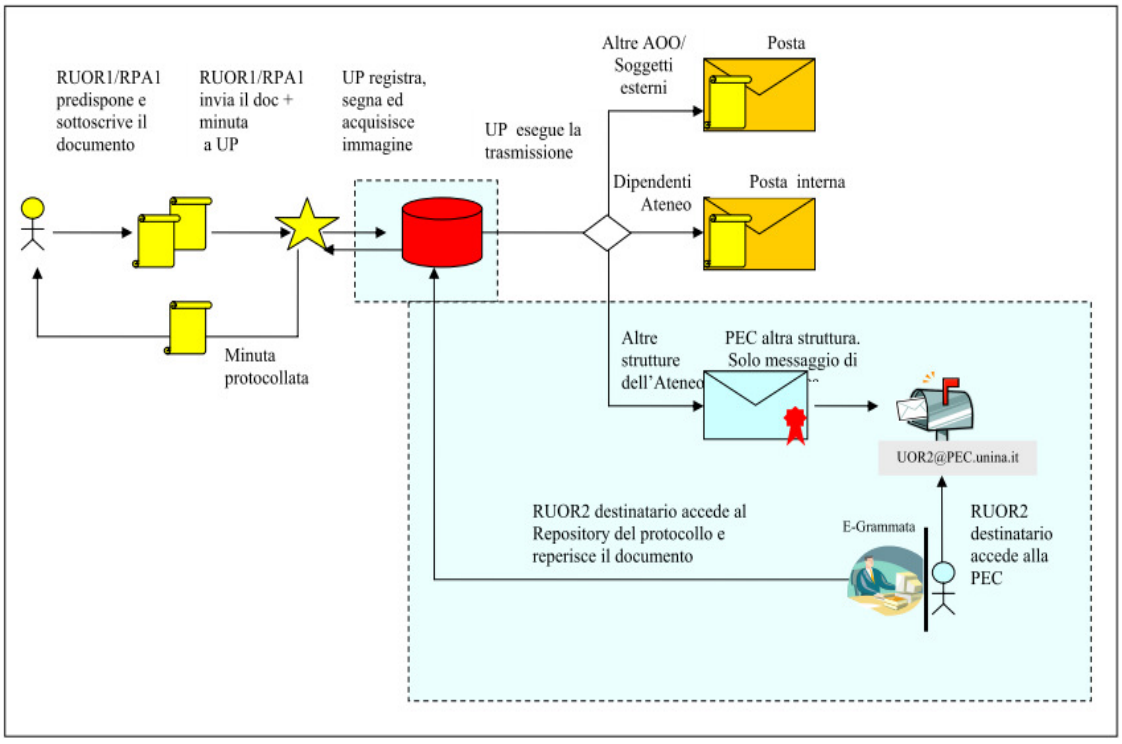
Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal UOP nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliate nel successivo capitolo 10.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

5.3.4. Trasmissione di documenti informatici

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno all'amministrazione).

Per la spedizione dei documenti informatici, l'Amministrazione si avvale del servizio di "posta elettronica certificata" UNINAPEC gestito dall'Università Il servizio, conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 che contiene il regolamento recante disposizioni per il relativo utilizzo è conforme al Regolamento di Ateneo emanato con DR 1614 del 11.05.2012. Tale servizio assicura la sicurezza del canale di comunicazione, fornisce certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.



Per quanto riguarda l'assegnazione di data certa ai documenti trasmessi via PEC, la AOO si avvale della marcatura temporale offerta dal PdP, in accordo con quanto previsto dal DPCM 30 marzo 2009 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici". Nel caso di trasmissione di documenti analogici, al messaggio PEC viene infatti allegata l'immagine del documento originale, provvista di segnatura di protocollo; se il documento è digitale, viene allegata la copia, ovvero – a seconda del procedimento – la copia conforme elettronica del documento digitale originale, in ogni caso completa dei dati di registrazione di protocollo e di contrassegno elettronico (il c.d. "timbro crittografico"). L'invio del messaggio PEC al destinatario è effettuato di norma dall'Ufficio mittente se dotato di PEC. In alternativa, procede l'UOP utilizzando la propria casella PEC.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

5.3.5. Trasmissione di documenti cartacei a mezzo posta

La sezione UOP-Smistamento posta presso ciascuna UOR provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici L'UOP conserva, temporaneamente, la minuta da restituire al mittente.

5.3.6. Affrancatura dei documenti in partenza

La sezione UOP-Smistamento posta della UOR competente provvede alle operazioni necessarie per l'invio della corrispondenza in partenza (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.). Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP.

5.3.7. Conteggi spedizione corrispondenza

L'UOP effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

5.3.8. Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno, e comunque in numero maggiore di tre, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

5.3.9. Trasmissione di documenti cartacei a mezzo telefax

Sul documento trasmesso via fax può essere apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale". Solo su richiesta del destinatario verrà trasmesso anche l'originale. Le ricevute della avvenuta trasmissione sono trattenute dagli UOR/UU/RPA che hanno formato il documento.

5.3.10. Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Gli UOR/UU/RPA, che effettuano la spedizione di documenti informatici o cartacei attraverso i propri UOP, curano anche l'archiviazione delle ricevute di ritorno, come già precedentemente illustrato.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

6. REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

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

6.1. Regole disponibili con il PdP

L'Amministrazione con il proprio PdP esegue lo smistamento e l'assegnazione dei documenti protocollati e segnati adottando le funzionalità di seguito illustrate.

L'attività di smistamento consiste nell'operazione di inviare un documento accettato dal servizio UOP-Smistamento posta alla UOR competente. Ciascuna UOR di primo livello dell'Amministrazione effettua mediante propri incaricati il servizio di accettazione e smistamento della posta in arrivo (cartacea o elettronica).

La corrispondenza indirizzata a ciascuna UOR viene consegnata dal servizio UOP-smistamento posta al responsabile della stessa UOR o ad un suo delegato alla sigla (denominato Responsabile Sigla, "RS", formalmente designato) per specifici procedimenti (ad esempio, quelli relativi alla didattica). Il Responsabile, dopo aver preso visione della corrispondenza, provvede ad accettarla e ad assegnarla ai propri UU/RPA, oppure, a chiederne la trasmissione ad altra UOR.

La registrazione di protocollo avviene solo a valle dell'assegnazione eseguita dal responsabile della UOR o da un suo delegato alla sigla. L'attività di assegnazione prevede che il responsabile della UOR (ovvero, il Responsabile di sigla) esegue la classificazione di primo livello in base al titolario vigente e l'assegnazione all'UOR/UU/RPA. Tali dati, assieme al documento sono utilizzati da UOP per la registrazione di protocollo del documento in cui gli assegnatari sono riportati come destinatari per competenza o per conoscenza della registrazione. Qualora non sia diversamente specificato, il nominativo RPA coincide con il responsabile dell'UOR/UU assegnataria.

L'UOR/UU/RPA, mediante PdP, provvede alla presa in carico del documento allo stesso assegnato, completo di segnatura (o timbro di segnatura).

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

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Nell'allegato 3 sono riportati le UOR dell'Amministrazione destinatari dello smistamento (eseguito, di norma da incaricati del servizio smistamento assegnati all'UOP) e autorizzate all'assegnazione (diretta o per mezzo di RS) a UU/RPA afferenti dei documenti ricevuti.

6.2. Corrispondenza di particolare rilevanza

Quando un documento pervenuto in Amministrazione appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è comunque in visione al Responsabile della UOR che provvede a individuare l'UOR/UU/RPA competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

6.3. Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'Amministrazione per via telematica, o comunque disponibili in formato digitale, sono direttamente disponibili all'attenzione della segreteria della UOR destinataria che provvede a smistare alla UOR competente per via telematica (utilizzando la posta elettronica o la PEC, a seconda dei casi), in modo tale da avviare il processo di sigla ed assegnazione da parte del Responsabile o del Responsabile di Sigla.

Come già riportato nei paragrafi precedenti, a valle dell'assegnazione, il documento informatico allegato al messaggio di posta – eventualmente l'intero messaggio di PEC in formato "eml" – viene inviato via posta elettronica al corrispondente UOP per la registrazione di protocollo.
L'UU/RPA competente ha notizia dell'arrivo della posta ad esso indirizzata tramite accesso al PdP e può quindi visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico. Più in particolare, in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare tutti i restanti assegnatari per competenza o per conoscenza.

La "presa in carico" dei documenti informatici viene registrata dal PdP in modo automatico e la data di ingresso dei documenti negli UOR competenti coincide con la data di assegnazione degli stessi.
I destinatari del documento (sia "per competenza" che "per conoscenza") lo ricevono esclusivamente in formato digitale.

6.4. Assegnazione dei documenti ricevuti in formato cartaceo

I documenti ricevuti dall'Amministrazione in formato cartaceo sono resi disponibili agli assegnatari, al pari di quelli digitali, comunque in formato elettronico, in quanto l'UOP acquisisce mediante scanner anche l'immagine del documento in fase di registrazione del documento stesso. Il primo assegnatario riceve anche il documento originale cartaceo, attraverso il sistema interno di smistamento e consegna della posta

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

dell'Amministrazione, assieme al rapporto di consegna che il responsabile UU/RPA restituisce all'UOP debitamente firmato.

L'UU/RPA competente ha notizia dell'arrivo del documento ad essa indirizzato tramite accesso al PdP e può quindi visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico. Più in particolare, in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare tutti i restanti assegnatari per competenza o per conoscenza;
- visualizzare i movimenti del documento;
- prendere in carico il documento;
- restituire il documento in caso di errata assegnazione;
- smistare/inviare il documento ad altra UO;
- prendere in carico il documento.

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

Il ritiro giornaliero della corrispondenza cartacea in arrivo da parte delle UOR in cui si articola l'Amministrazione (AOO) avviene presso le UOP riceventi di cui è provvista ciascuna UOR.

6.5. Modifica delle assegnazioni

Di seguito, si riporta il flusso della presa in carico, con particolare riguardo alla gestione del cambio assegnatario, con riferimento al caso (più complesso) della UOR Amministrazione Centrale.

Il flusso operativo ordinario

Ciascun ufficio (UU) si collega con frequenza almeno giornaliera al PdP e verifica la presenza di documenti da prendere in carico.

Prima di prendere in carico i documenti presenti in "lista di lavoro", l'ufficio controlla che il documento sia siglato, cioè che gli sia stato inviato dalla propria UOR di diretta afferenza (oppure, dalla Direzione Generale nel caso degli uffici dell'Amministrazione Centrale).

In caso affermativo (documento siglato) l'ufficio potrà:

- prendere in carico il documento, se il documento è di propria competenza;

oppure,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- richiedere il cambio assegnatario, se il documento non è di propria competenza.

  - **La presa in carico**

Se il documento è siglato ed è di competenza dell'ufficio, l'UU prende in carico il documento.

  - **La richiesta del cambio assegnatario**

Se il documento è siglato, ma non è di competenza dell'ufficio, l'UU richiede il cambio assegnatario.

Pertanto, l'UU:

- Smisterà il documento alla struttura del Responsabile di Sigla mittente (Amministrazione Centrale o Ripartizione o, più in generale, alla UOR gerarchicamente superiore), senza prenderlo in carico;
- Se primo assegnatario, invierà al Responsabile di Sigla anche il documento cartaceo.

Il Responsabile di Sigla dovrà quindi collegarsi al sistema di Protocollo Informatico, accedere alla propria "lista di lavoro" e smistare il documento al nuovo assegnatario. Se il cambio è relativo al primo assegnatario, il Responsabile di Sigla dovrà, infine, stampare il "rapporto di consegna" e trasmetterlo, insieme al documento cartaceo originale all'Ufficio di Protocollo per le ordinarie operazioni di consegna al nuovo ufficio destinatario.

  - **La gestione del documento non siglato**

Se il documento non è siglato, l'UU, sempre accedendo alla propria "lista di lavoro", dovrà controllare se:

1. il documento ha tra i destinatari di registrazione anche l'Amministrazione Centrale. In tal caso, attenderà la ricezione della propria copia siglata (Tale copia sarà elettronica per gli assegnatari diversi dal primo, cartacea ed elettronica solo per il primo assegnatario);
   oppure,

a. il documento non ha tra i destinatari anche l'Amministrazione Centrale. In tal caso, l'ufficio smisterà la propria copia elettronica all'Amministrazione Centrale per far avviare il procedimento di sigla ed assegnazione ed invierà all'Amministrazione Centrale anche l'eventuale documento cartaceo.

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

7. UO RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E DI TENUTA DEI DOCUMENTI

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno dell'Amministrazione.
In base al modello organizzativo adottato dall'Amministrazione (si veda il par. 1.4 del presente MdG), nell'allegato 3 è riportato l'elenco delle unità organizzative di I livello responsabili delle attività di registrazione del protocollo (UOR), effettuate mediante il servizio UOP costituito da un'unità organizzativa dedicata, oppure da postazioni di incaricati afferenti alla UOR e abilitati al protocollo.

Per quanto riguarda l'organizzazione e la tenuta dei documenti dell'Amministrazione all'interno di essa, sono istituiti: il servizio archivistico, il servizio di coordinamento del protocollo informatico, a seguire, il servizio per la conservazione sostitutiva e sono definite le strutture dedicate alla conservazione dei documenti.

I servizi in argomento sono stati identificati e formalizzati prima di rendere operativo il servizio di gestione informatica del protocollo, dei documenti e degli archivi.

7.1. Servizio di protocollo

L'Ateneo è suddiviso, ai fini del protocollo e della gestione dei flussi documentali in UOR che utilizzano, in modo coordinato e omogeneo i servizi informativi e le risorse infrastrutturali messe a disposizione dall'Ateneo, nonché ne condividono i regolamenti e le policy, adottatati in coerenza e nel rispetto della normativa vigente. Ciascuna UOR è dotata di un proprio servizio UOP per la gestione del protocollo e dell'archivio corrente. I compiti dell'UOP sono finalizzati allo svolgimento degli adempimenti in materia di protocollo informatico e di gestione della corrispondenza della UOR di appartenenza, attraverso le attività di:

- segnatura, classificazione e registrazione di protocollo dei documenti cartacei e digitali dell'Amministrazione Centrale, in partenza ed in arrivo;
- annullamento delle registrazioni di protocollo;
- copia e ricerca dei documenti protocollati;
- inoltro della corrispondenza cartacea a mezzo posta;
- acquisizione della posta cartacea in arrivo e smistamento dei documenti protocollati agli uffici competenti.

In particolare, l'Ufficio Protocollo dell'Amministrazione Centrale è stato recentemente riorganizzato: il suo decreto di istituzione è il DD/2013/11 del 2.1.2013.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

7.2. Servizio archivistico

La gestione dell'archivio di deposito dei documenti della AOO è centralizzata ed è affidata all'Ufficio Archivio, afferente all'Amministrazione Centrale dell'Ateneo ed istituito con DD/2013/11 del 2.1.2013.

I compiti dell'Ufficio sono finalizzati alla salvaguardia, alla tutela, alla valorizzazione e promozione del patrimonio documentale dell'Università cartaceo ed informatico, attraverso le attività di:

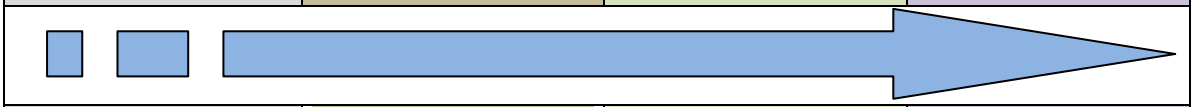
- acquisizione dai responsabili dei procedimenti amministrativi degli atti e dei documenti di rispettiva competenza, ai fini della archiviazione;
- gestione dell'archivio di deposito;
- recupero ed esibizione della documentazione a fronte di specifiche e motivate richieste da parte degli uffici competenti;
- predisposizione della regolamentazione e delle relative procedure operative per lo scarto dei documenti archiviati e per la conservazione digitale dei documenti e dei fascicoli formati con strumenti informatici, in ottemperanza con quanto prescritto dalla normativa vigente in materia.

7.3. Servizio di coordinamento del protocollo informatico

Per garantire l'adozione di prassi operative coordinate e il corretto utilizzo degli strumenti informatici, come già illustrato nel paragrafo 1.5, l'Ateneo ha organizzato e istituito con DD n. 3 del 7.1.2009 (riportato in allegato 4) il servizio di "Coordinamento del Protocollo informatico". Lo schema organizzativo di riferimento è il seguente:

Coordinamento del Protocollo informatico
▪ Predispone lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo; ▪ Provvede alla pubblicazione del manuale anche per via telematica; ▪ Propone i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, e, più in generale, dei protocolli diversi dal protocollo informatico; ▪ Organizza il sistema di gestione dei flussi documentali; ▪ Collabora alla messa a punto 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: a) il responsabile dei sistemi informativi automatizzati; b) il titolare dei trattamenti dei dati di cui al dlgs. n. 196/03; c) il responsabile del servizio archivistico; d) il responsabile della conservazione sostitutiva. ▪ Ai fini della corretta gestione dell'intero ciclo di vita dei documenti informatici, supporta il Direttore Generale per il coordinamento e l'integrazione delle attività svolte dall'UOP delle singole UOR, dal C.S.I., dal Servizio Archivio (per quanto attiene al trattamento informatico dei documenti archiviati) e dal Servizio di Conservazione.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Responsabile UOR – Servizio UOP	Responsabile S.I.	Responsabile Archivio	Responsabile Conservazione
			
▪ Attribuisce il livello di autorizzazione (ruolo) di ciascun addetto all'accesso alle funzionalità offerte dall'applicazione di Protocollo Informatico provvedendo a distinguere competenze e ruoli in base alle abilitazioni alla consultazione, all'inserimento, alla modifica e alla cancellazione delle informazioni; ▪ Garantisce il rispetto della normativa vigente durante le operazioni di registrazione e di segnatura di protocollo; ▪ Autorizza le operazioni di annullamento della registrazione di protocollo; ▪ Autorizza l'apertura e la chiusura del registro di emergenza ed è responsabile della corretta tenuta di tale registro; ▪ Vigila	▪ Gestisce il corretto funzionamento del sistema, secondo adeguati livelli di servizio e caratteristiche funzionali e tecniche concordate con RSP; ▪ Amministra il piano della sicurezza informatica definito con RSP; ▪ Garantisce la corretta produzione e la custodia del registro giornaliero di protocollo; ▪ Cura le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e, comunque entro le ventiquattro ore dal blocco delle attività; ▪ Stabilisce i criteri minimi di sicurezza informatica del sistema; ▪ Conserva le copie di salvataggio delle informazioni del	▪ Stabilisce i livelli di accesso ai documenti archivistici e regolamenta le forme di consultazione interna ed esterna dell'archivio, nel rispetto della normativa sulla tutela della riservatezza dei dati personali; ▪ Organizza la fase di versamento dei documenti dagli Uffici all'Archivio generale; ▪ Cura e garantisce la conservazione dell'archivio nella fase di deposito; ▪ Predispone il piano di conservazione dei documenti, prescritto dal DPR 445/2000,art. 68; ▪ Predisporne il massimario di scarto; ▪ Effettua la selezione periodica dei documenti e procedere allo scarto o al trasferimento nella separata sezione	▪ Organizza e gestisce il trasferimento su supporto informatico rimovibile delle informazioni di protocollo relative ai fascicoli che fanno riferimento a procedimenti conclusi; ▪ Dispone, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

sull'osservanza della normativa vigente in materia da parte del personale afferente alla UOR.	sistema.	d'archivio del materiale destinato alla conservazione permanente.	

7.4. Servizio della conservazione elettronica dei documenti

Tale servizio sarà organizzato nell'ambito del Centro di Ateneo per le Biblioteche (CAB), così come previsto dal Regolamento del Sistema bibliotecario di Ateneo e del Centro di Ateneo per le Biblioteche. In particolare, il CAB definisce gli standard e le modalità di archiviazione della documentazione prodotta in formato digitale.

Ai fini dell'organizzazione e dell'avvio del processo di conservazione a norma dei documenti digitali, in attuazione dell'Art. 44 comma 1 del d.lgs. 82/2005 s.m.i. (il "Codice dell'Amministrazione Digitale"), con Decreto del Direttore Generale n. 1071 del 24.07.2013, l'Ateneo ha provveduto alla nomina del Responsabile della Conservazione. Il Responsabile della Conservazione dovrà, in collaborazione con il Responsabile del Servizio di Coordinamento del Protocollo Informatico, alla redazione del Manuale di Conservazione, strumento fondamentale per tutto il sistema di conservazione, in quanto ne descrive i processi di gestione e la sua compiuta attuazione garantisce la tenuta a norma del sistema stesso ed illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

7.4.1. Archiviazione ottica dei documenti analogici

Il responsabile del servizio archivistico, valutati i costi ed i benefici, può proporre l'operazione di conservazione sostitutiva dei documenti analogici su supporti di memorizzazione sostitutivi del cartaceo in conformità alle disposizioni vigenti.

7.4.2. Archiviazione ottica dei documenti digitali

Il processo di conservazione sostitutiva dei documenti informatici, anche sottoscritti, inizia con la memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento di tale processo. Il processo di riversamento sostitutivo di documenti informatici avviene mediante memorizzazione su altro supporto magneto-ottico a norma e termina con l'apposizione sull'insieme dei documenti o su una evidenza informatica contenente

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo. Qualora il processo riguardi documenti informatici sottoscritti è richiesta anche l'apposizione del riferimento temporale e della firma digitale, da parte del Responsabile della Conservazione, pubblico ufficiale autorizzato ad attestare la conformità di quanto riversato al documento d'origine.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

8. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

8.1. Documenti esclusi

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 28 dicembre 2000. n. 445:

- gazzette ufficiali,
- bollettini ufficiali
- notiziari della pubblica amministrazione
- note di ricezione delle circolari e altre disposizioni
- materiali statistici
- atti preparatori interni
- giornali
- riviste
- libri
- materiali pubblicitari
- gli inviti a manifestazioni
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione

Sono inoltre escluse dalla registrazione di protocollo tutte le tipologie di documenti riportate nell'**allegato 10**.

8.2. Documenti soggetti a registrazione particolare

Nell'ambito della gestione del Protocollo Informatico, al fine di garantire particolari forme di riservatezza e di accesso controllato al sistema, è istituito il Protocollo particolare, repertorio del Protocollo generale utilizzato, a discrezione del Rettore e/o del Direttore Generale, per la registrazione:

1. di documenti legati a vicende di persone o a fatti privati o particolari;
2. di documenti di carattere politico e di indirizzo di competenza del Rettore e del Direttore Generale che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
3. di documenti di carattere politico o gestionale dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
4. delle tipologie di documenti individuate dalla normativa vigente (in particolare dall'art. 24 della legge 7 agosto 1990, n. 241, dall'art. 8 del DPR 27 giugno 1992,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

n. 352, dalla serie di norme collegate al DLGS 30 giugno 2003, n. 196, e dal DR 2386 del 17.6.1998 recante le regole di attuazione della citata legge 241/90).

L'elenco dei atti registrati nel registro di protocollo particolare è riportato in **allegato 11**.

Tali documenti, pur appartenendo al Protocollo generale, sono trattati in forma particolare, sia in fase di registrazione, che di scansione ottica che di consultazione, con garanzia di livelli di accesso riservato.

I documenti dell'archivio particolare divengono consultabili alla scadenza dei termini indicati dalla normativa vigente, ovvero, in mancanza dei termini, alla data fissata dal Rettore e/o dal Direttore Generale. Motivate richieste di consultazione potranno essere accolte prima della scadenza dei termini secondo quanto previsto dalla normativa in materia di accesso ai documenti amministrativi.

8.3. Norme di utilizzo del protocollo particolare

8.3.1. La registrazione di protocollo

I documenti particolari sono dotati di un numero di protocollo progressivo nell'ambito del Protocollo generale (secondo quanto sancito dal DPR 445/2000, art. 57) e unico, secondo quanto enunciato dal DPCM 31.10.2000 art.3.1, comma d). Contestualmente, ad ogni nuova registrazione particolare è assegnato dal PdP un codice univoco e progressivo anche nel repertorio "**PP**".

Le registrazioni di protocollo particolare, complete delle immagini dei documenti acquisiti, sono eseguite su una postazione di lavoro presso la Segreteria della Direzione Generale da utenti autorizzati all'utilizzo di tale funzionalità del PdP.

La visualizzazione delle registrazioni particolari, al pari della registrazione, è consentita solo agli utenti all'uopo autorizzati.

8.3.2. Acquisizione dell'immagine del documento

L'immagine del documento, può essere acquisita, facoltativamente, mediante scanner direttamente dalla postazione presso la Segreteria di Direzione, contestualmente alla registrazione di protocollo oppure in una fase differita, comunque entro la giornata.

8.3.3. Stampa e tenuta del registro particolare

La stampa del registro particolare è eseguita dal Servizio Coordinamento del Protocollo Informatico, in automatico, nell'ambito della procedura di stampa del registro giornaliero. Nella stampa del registro, per le registrazioni appartenenti al repertorio PP così come per quelle di protocollo generale, compaiono la data, il numero di

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

protocollo, l'oggetto ed il mittente/destinatario di ciascun documento particolare protocollato. Tale stampa, prodotta in automatico, viene sottoposta alle procedure di salvataggio e archiviazione da parte di RSI.. L'accesso alla cartella di sistema contenente i file prodotti dalla funzionalità di stampa dei registri giornalieri è consentita esclusivamente agli Amministratori di Sistema del PdP. Il processo di gestione del salvataggio periodico su supporto rimovibile del registro PP è parte integrante di quello del registro di Protocollo Generale descritto nel paragrafo 10.10.2.

8.3.4. Annullamento di registrazioni di protocollo particolare

L'annullamento di registrazioni effettuate nell'ambito del Protocollo particolare deve essere eseguito, previa richiesta scritta a firma del Direttore Generale, dall'Ufficio di Segreteria di Direzione. La richiesta deve contenere le indicazioni sul numero di protocollo da annullare e la motivazione del provvedimento. Le operazioni di annullamento da eseguire nel PdP sono le stesse utilizzate per l'annullamento di registrazioni di protocollo generale.

8.3.5. Abilitazione all'accesso a dati e funzioni

L'utilizzo delle funzionalità per la gestione del protocollo particolare e l'accesso alle informazioni collegate ai documenti particolari sono consentiti esclusivamente al Rettore, al Direttore Generale e ai loro incaricati, mediante la creazione di appositi profili utente.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

9. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

9.1. Protezione e conservazione degli archivi pubblici

9.1.1. Generalità

Il presente capitolo illustra le caratteristiche generali del sistema di classificazione dei documenti e di formazione del fascicolo. Le informazioni relative alla tenuta e alla conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli, saranno oggetto di manuali e documentazione predisposta dai Responsabili preposti alla gestione del contesto archivistico e della conservazione, secondo un approccio comunque integrato e coordinato con quanto riportato nel presente Manuale. L'obiettivo del presente documento, infatti, come evidenziato in premessa, è di fornire un'esaustiva trattazione per quanto attiene alla gestione del protocollo informatico, dell'archivio elettronico e dei flussi documentali informatici. Relativamente alle tematiche dell'archiviazione dei documenti analogici e della conservazione dei documenti analogici e digitali, il presente Manuale si limita infatti a riportare, ove previsto, indicazioni di massima, comunque utili a fornire un quadro d'insieme dell'organizzazione dell'Ateneo per la tutela e la conservazione del proprio patrimonio documentale, rinviando comunque alla documentazione tematica redatta dai competenti uffici e servizi.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

Il piano di conservazione, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'Amministrazione nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio.

Il titolario e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'Amministrazione. Spetta ai vertici dell'Amministrazione medesima adottare il titolario e il piano di conservazione con atti formali.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Come già riportato nel paragrafo 1.10, con riferimento al titolario di classificazione, è opportuno far presente che, all'avvio del PdP il 1 gennaio 2007, l'Ateneo ha adottato, in via transitoria il Titolario utilizzato fino al 31.12.2006 dalla Amministrazione Centrale. Successivamente, con Ordine di Servizio n. 159 del 3 giugno 2008, l'Ateneo ha quindi adottato il nuovo Titolario di classificazione, riportato (nella sua versione emendata in data 22.10.2013) in **allegato 12**.

9.1.2. Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici sono beni assoggettati al regime dei beni demaniali e, in quanto tali, inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'Amministrazione, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità. Il trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della Direzione generale per gli archivi. L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della Direzione generale per gli archivi. Relativamente agli enti pubblici non statali l'autorizzazione per l'eventuale rimozione e/o trasferimento dell'archivio, è demandata, per delega della Direzione Generale degli archivi, alle Sovrintendenze archivistiche.

Per l'archiviazione e la custodia nella sezione di deposito o storica dei documenti contenenti dati personali, si applicano in ogni caso le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che convenzionali.

9.2. Titolario o piano di classificazione

9.2.1. Titolario

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente. Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo dell'Amministrazione.
Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali. L'aggiornamento del titolario compete esclusivamente al vertice dell'Amministrazione. La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno. Dopo ogni modifica del titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione. Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi. Inoltre, per ogni modifica di una voce viene riportata la data di introduzione e la data di variazione. Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo titolario e valgono almeno per l'intero anno. Il sistema PdP adottao dall'Ateneo, inoltre, consente di registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

Il titolario è elaborato da RSP e, a valle della revisione effettuata da un gruppo di lavoro individuato dal Direttore Generale, viene emanato con apposito decreto del Direttore Generale.

Il titolario adottato dall'Amministrazione è pubblicato nella sua versione aggiornata all'indirizzo:

http://www.praxis.unina.it/protocollo-sistema-ateneo

9.2.2. Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Amministrazione. Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.

Tutti i documenti ricevuti e prodotti dagli UOR dell'Amministrazione, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario. Il sistema PdP consente di specificare un diverso indice di titolazione per ciascun destinatario (competenza o conoscenza) di registrazione.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

9.3. Fascicoli elettronici

9.3.1. Fascicolazione dei documenti

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

Il sistema è predisposto per abilitare gli utenti del PdP destinatari di registrazioni di protocollo a modificare il fascicolo in cui è stato inserito il documento in fase di registrazione di protocollo.

9.3.2. Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'ente, il soggetto preposto (quale, ad esempio, RPA, RSP, responsabile del servizio archivistico addetto alla protocollazione, etc.) provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione, (cioè titolo, classe, sottoclasse, etc.);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'Amministrazione;
- data di apertura del fascicolo;
- UOR;
- collocazione fisica, di eventuali documenti cartacei;
- collocazione logica, dei documenti informatici;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. Le informazioni di cui sopra, compaiono sulla camicia del fascicolo.

Attualmente, l'apertura di un fascicolo elettronico è eseguita in automatico dal PdP, in base alla voce di classificazione del documento, qualora per l'anno di riferimento non esista già un fascicolo relativo allo stesso procedimento amministrativo per la data UOR protocollante.

9.3.3. Chiusura del fascicolo

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

La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura. Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo 9.3.2., primo capoverso, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

9.3.4. Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'Amministrazione, l'UOR abilitata all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stessa debba essere ricollegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce a un nuovo affare o procedimento per cui è necessario aprire un nuovo fascicolo .

A seconda delle ipotesi, si procede come segue:

- Se il documento si ricollega ad un affare o procedimento in corso, l'addetto:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato;
  - invia il documento all'UOR cui è assegnata la pratica (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).
- Se il documento dà avvio ad un nuovo fascicolo, il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo;
  - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;
  - assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
  - invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

Come già detto nel paragrafo precedente, alla data, l'operazione di assegnazione di un documento ad fascicolo è svolta in automatico, per ciascuna copia prodotta a fronte di ogni registrazione di protocollo, dal PdP, sulla base della voce di titolazione del documento attribuita a ciascuna copia. Il fascicolo è attualmente sempre assegnato alla AOO e gli utenti del PdP potranno accedere a tutti i fascicoli che contengono almeno un documento a cui sono autorizzati ad accedere (in quanto destinatari di registrazione di protocollo o di copia per competenza o per conoscenza). Inoltre, non sono gestiti sottofascicoli. Tutte le operazioni precedentemente illustrate saranno invece previste nel sistema documentale.

9.3.5. Modifica delle assegnazione dei fascicoli

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore di UU che effettua la modifica con la data e l'ora dell'operazione. Attualmente, nel PdP la richiesta di modifica viene consentita solo agli incaricati autorizzati che possono modificare la voce di classificazione per un dato documento registrato e, quindi, modificarne di conseguenza il fascicolo, oppure richiedere l'inserimento del documento in diverso fascicolo, a patto che il fascicolo sia creato non chiuso e di averne l'accesso. Tutte le operazioni di tipo generale precedentemente illustrate sono invece previste nel sistema documentale, di prossimo avvio.

9.3.6. Repertorio dei fascicoli

I fascicoli, sono annotati nel repertorio dei fascicoli.

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività .

Nel repertorio sono indicati:

- la data di apertura del fascicolo;
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc.);
- il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sottofascicoli e inserti);
- l'annotazione sullo status relativo al fascicolo, se cioè sia ancora una "pratica" corrente, o se abbia esaurito la valenza amministrativa immediata e sia quindi da mandare in deposito, oppure, infine, se sia da scartare o da passare all'archivio storico;
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio di storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

9.4. Serie archivistiche e repertori

9.4.1. Serie archivistiche

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

documenti (es. le determinazioni, i contratti, i registri di protocollo) oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono (es. i fascicoli personali, le pratiche di finanziamento e in generale le pratiche attivate dall'Amministrazione nello svolgimento dell'attività istituzionale).

Le serie documentarie sono formate dai registri e dai relativi fascicoli compresi in un arco d'anni variabile.

I fascicoli subiscono il processo di selezione e scarto dei documenti; le serie così composte, faranno parte, successivamente, della sezione storica dell'archivio[3].

9.4.2. Repertori e serie archivistiche

I documenti soggetti a registrazione progressiva ed omogenea per tipologia di affare a cui si riferiscono, come i verbali di esame, le delibere degli organi di governo dell'Amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.

Con riguardo alla gestione dei documenti cartacei, è previsto per ogni verbale, delibera, determinazione, decreto, ordinanza e contratto siano, di norma, prodotti almeno due originali di cui:

- uno viene inserito nel registro di repertorio con il numero progressivo di repertorio;
- l'altro, viene conservato nel relativo fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- ad un codice di protocollo generale, a seconda della tipologia del repertorio stesso;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso. Il repertorio è costantemente aggiornato.

[3] riferimento: art.41 comma 3 D.Lgs. 42/2004; DPR 8 gennaio 2001 n.37, art.10, *regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di vigilanza sugli archivi e per lo scarto dei documenti degli uffici dello Stato* (entrambe le disposizioni si riferiscono agli Archivi di Stato e dunque agli archivi statali, ma per prassi si applicano anche agli archivi pubblici non statali, per i quali non esiste una norma analoga; lo scarto dei documenti degli archivi pubblici e degli archivi privati dichiarati di notevole interesse storico è disciplinato dall'art.21, comma 1, lett.*d*) dello stesso decreto legislativo 42/2004)

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

All'interno dell'Amministrazione sono istituiti i repertori generali indicati **nell'allegato 13**.

9.4.3. Versamento dei fascicoli nell'archivio di deposito

Documenti analogici

La formazione dei fascicoli (virtuali o tradizionali), delle serie e dei repertori è una funzione fondamentale della gestione archivistica ed è compito istituzionalmente assegnato al Capo dell'Ufficio Archivio dell'Amministrazione Centrale (nel seguito, RSA). Periodicamente, e comunque almeno una volta all'anno, RSA provvede a trasferire i fascicoli e le serie documentarie relativi ai procedimenti conclusi in un apposita sezione di deposito dell'archivio generale costituito presso l'Amministrazione.
Per una regolare e costante "alimentazione" dell'archivio di deposito lo stesso responsabile dell'archivio stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi UOR/UU dell'Amministrazione all'archivio di deposito.
Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori generali.
La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.
Prima di effettuare il conferimento di cui sopra, il RPA/UU procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- della corretta indicazione della data di chiusura sulla camicia del fascicolo;

Il RPA/UU provvede inoltre:

- allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli e controllato l'aggiornamento del relativo repertorio, RSA predispone un elenco di "versamento" da inviare al servizio archivistico. Copia di detto elenco viene conservata dal responsabile che ha versato la documentazione.

Documenti digitali

I documenti amministrativi digitali (sottoscritti cioè con firma digitale) sono immodificabili ed integri. Pertanto, qualora siano registrati e custoditi nel PdP, è

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

compito dell'RSP, anche in accordo con la bozza predisposta da DigitPA (oggi Agenzia per l'Italia digitale) delle "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44 –bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005", con frequenza e temporizzazione da definirsi a valle dell'avvio del servizio di conservazione, procedere a produrre i pacchetti di versamento. Più in dettaglio, i documenti digitali custoditi nel PdP saranno periodicamente versati nel sistema di conservazione a cura del RSP che:

1. provvede a generare, per uno o più documenti informatici, un pacchetto di versamento nelle modalità e con i formati concordati con il responsabile della conservazione e previsti dal manuale di conservazione redatto e tenuto dal Responsabile della Conservazione;
2. stabilisce, per le diverse tipologie di documenti, in conformità con le norme vigenti in materia, con il sistema di classificazione e con il piano di conservazione, i tempi entro cui i documenti debbono essere versati in conservazione;
3. verifica il buon esito dell'operazione di versamento tramite il rapporto di versamento prodotto dal sistema di conservazione.

A valle della diffusione del sistema documentale, tali operazioni saranno eseguite direttamente a partire dal sistema documentale di Ateneo sui documenti e fascicoli preventivamente "chiusi", quindi segnalati per la conservazione e pertanto posti nello stato "versabile" da parte dell'UOR/UU/RPA proprietario e dunque tenutario del fascicolo o documento da versare.

9.4.4. Verifica della consistenza del materiale riversato nell'archivio di deposito

L'ufficio ricevente esegue il controllo del materiale riversato. Il servizio archivistico dell'Amministrazione riceve agli atti soltanto i fascicoli con materiale ordinato e completo. Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito agli UOR/UU/RPA tenutari dell'archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie. Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, il responsabile degli UOR deposita il fascicolo dichiarando ufficialmente che è incompleto e si assume la responsabilità della trasmissione agli atti.

Ricevuti i fascicoli e controllato il relativo elenco, RSA firma per ricevuta l'elenco di consistenza.

Nel caso di versamento di contenuti digitali versati a partire dal PdP, come detto nel paragrafo precedente, è il RSP ad eseguire la verifica del rapporto di versamento prodotto in automatico dal sistema di conservazione. Se il pacchetto contenente il documento oppure il fascicolo è invece prodotto su richiesta diretta della UOR/UU/RPA proprietario dell'archivio digitale corrente gestito mediante il sistema documentale.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

9.5. Scarto, selezione e riordino dei documenti

Anche se la trattazione sarà effettuata dai Responsabili dei servizi archivistici e di conservazione in documenti specifici, verificati ed autorizzati nelle sedi opportune, di seguito si riportano le linee guide generali già adottate o programmate dall'Amministrazione, in accordo con la normativa e le regole tecniche vigenti in materia.

9.5.1. Operazione di scarto

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'Amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.

La legge impone all'Amministrazione l'uso di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio.

Il massimario viene proposto dal RSA alla direzione generale degli archivi del Ministero dei beni e delle attività culturali per il tramite della Soprintendenza ai beni archivistici e viene autorizzato con atto formale dall'organo competente dell'Amministrazione. Le operazioni di selezione e scarto sono effettuate, sotto la vigilanza del RSA, a cura degli addetti del servizio archivistico. I documenti e gli atti sottoposti a procedura di scarto sono devoluti gratuitamente secondo quanto stabilito dal Decreto del Presidente della Repubblica del 8 gennaio 2001, n. 47 art. 8[4].

Tale massimario, a valle della sua emanazione, viene utilizzato anche da RSP e dalle UOR/UU/RPA per impostare la data di scadenza dei documenti e dei fascicoli digitali riportata nel pacchetto di versamento che determina l'avvio automatico della procedura di scarto.

[4] Fino al 2001 la materia era regolata dal RDL 10 agosto 1928 n.2034 art.16, e successive modifiche, che prevedeva la cessione obbligatoria gratuita alla CRI. Tale disposizione fu abrogata dal DPR 8 gennaio 2001 n.37, art.10, (regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di vigilanza sugli archivi e per lo scarto dei documenti degli uffici dello Stato). L'art. 8 del DPR 47/2001 stabilisce che le modalità di cessione degli atti vengono stabilite da ciascuna Amministrazione; esso dunque non configura un obbligo di cessione alla CRI, conferendo anzi all'Amministrazione procedente facoltà di scelta tra la stessa Croce Rossa e le organizzazioni di volontariato. Nel maggio 2001, con decreto del Ministro del Tesoro (DM 21 maggio 2001) è stata rinnovata la concessione alla CRI la concessione per il ritiro del materiale destinato allo scarto, prevista dalla vecchia disposizione del 1928, nel frattempo abrogata. Tale concessione, nel nuovo quadro normativo, deve considerarsi come conferita *in via non esclusiva*.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

9.5.2. Conservazione del materiale presso la sezione di deposito dell'archivio

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita dall'Amministrazione e consiste nella schedatura dei materiali e nell'organizzazione delle schede.
L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (scatole, pallets, etc) che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti.

9.5.3. Versamento dei documenti nella sezione separata dell'archivio di deposito o generale: sezione detta "archivio storico".

Gli enti pubblici, territoriali e non, trasferiscono al proprio archivio storico, ossia alla sezione separata dell'archivio di deposito o generale, i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.

I trasferimenti vengono effettuati dopo il completamento delle operazioni di scarto.

Presso l'archivio storico i documenti vengono inventariati al fine della conservazione, consultazione e valorizzazione.

9.6. Consultazione e movimentazione dell'archivio corrente, di deposito e storico

9.6.1. Principi generali

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può pervenire dall'interno dell'Amministrazione oppure da utenti esterni all'Amministrazione, per scopi giuridico-amministrativi o per scopi storici.

9.6.2. Consultazione ai fini giuridico-amministrativi[5]

Il diritto di accesso ai documenti è disciplinato dall'art.24 della legge 7 agosto 1990, n.241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15

9.6.3. Consultazione per scopi storici

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata dal regolamento emanato da ciascuna Amministrazione. La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'Interno (a norma dell'art. 125 del decreto legislativo 22 gennaio 2004, n.42) o per regolamento emanato dalla stessa Amministrazione. È possibile l'ammissione alla consultazione dei documenti riservati, previa

[5] Il riferimento è alla legge 241/90 e successive modifiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);

- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

9.6.4. Consultazione da parte di personale esterno all'Amministrazione:

La domanda di accesso ai documenti viene presentata all'Ufficio relazioni con il pubblico (URP), che provvede a smistarla al servizio archivistico.

L´URP mette a disposizione appositi moduli, pubblicati all'indirizzo http://www.unina.it/ateneo/attiNorme/modulistica/urp.jsp.

Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla soprintendenza per i beni archivistici territorialmente competente, con apposito modulo da questa predisposto.

Le domande vengono evase durante gli orari di apertura al pubblico dell'URP e dell'archivio con la massima tempestività e comunque non oltre 30 giorni dalla presentazione.

Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale. In tal caso il responsabile del servizio di conservazione provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.

L´ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico. La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio può avvenire previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'Amministrazione.

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni. Le disposizioni dei commi precedenti si applicano anche alla consultazione di archivi storici presso le pubbliche amministrazioni che non si siano ancora dotate di apposito servizio per l'apertura alla pubblica consultazione degli archivi.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

9.6.5. Consultazione da parte di personale interno all'Amministrazione

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i propri fascicoli conservati nella sezione archivistica di deposito o in quella separata (archivio storico). Maggiori dettagli sulle modalità di gestione delle richieste di consultazione sono contenuti nell'**allegato 9**.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio del medesimo UOR/UU od altro UOR/UU avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.

Un esemplare della richiesta di consultazione viene conservata all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio. Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compare la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.

Il Responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, rispettandone la sedimentazione archivistica e il vincolo.

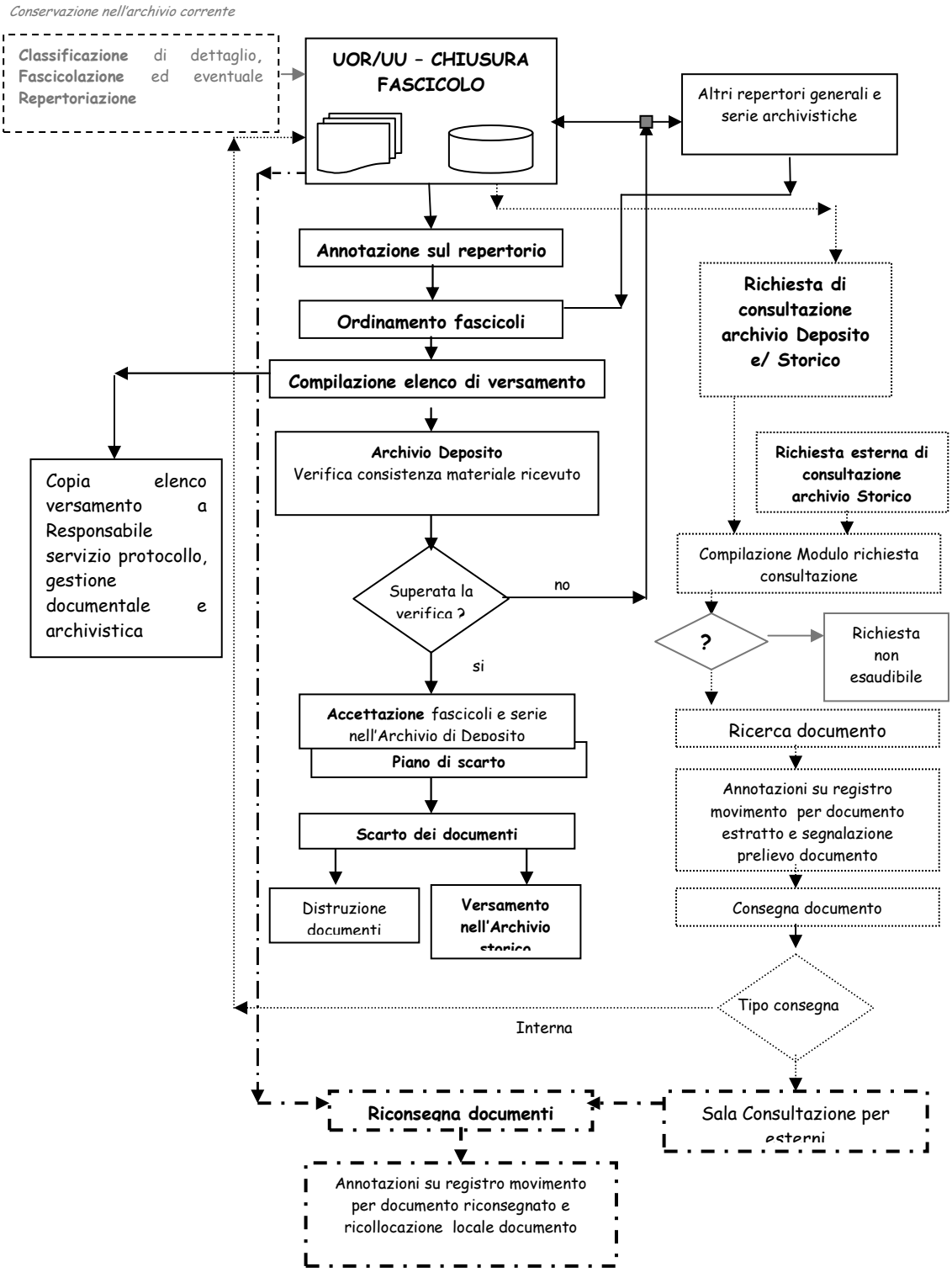
Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'Amministrazione.

In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

9.6.6. Schematizzazione del flusso dei documenti all'interno del sistema archivistico

Nella pagina seguente viene riportata una rappresentazione grafica sintetica del complesso delle attività, delle norme e delle responsabilità illustrate nel presente capitolo che, nella loro totalità, costituiscono funzione strategica dell'Amministrazione.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

10.1. Unicità del protocollo informatico

Nell'ambito dell'Amministrazione, il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo, centralizzato o distribuito delle UOP, adottato dall'Amministrazione medesima. Nel caso dell'Università degli Studi di Napoli Federico II, come si è detto già nel I capitolo, il modello organizzativo adottato dall'Ateneo è distribuito.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Il numero di protocollo è costituito da sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'Amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

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.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.2. Registro giornaliero di protocollo

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

La descrizione della modalità di estrazione e produzione del registro informatico di protocollo è riportata nel paragrafo 10.10.2.

10.3. Registrazione di protocollo

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

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

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

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

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

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili. Tali dati facoltativi sono descritti nei paragrafi seguenti.

10.3.1. Documenti informatici

Ai sensi del Regolamento di Ateneo in materia di Firma Digitale (D.R. 4064 del 31/10/2006), tutti i documenti informatici che rappresentano atti amministrativi dell'Università devono essere firmati digitalmente e registrati nel sistema di protocollo informatico. Il sistema di Protocollo Informatico, associando al documento un insieme di attributi di registrazione univoci ed immodificabili, garantisce – tra l'altro – la data certa di formazione dell'atto e la memorizzazione dell'esito delle verifiche sulla

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

autenticità ed integrità del documento digitale all'atto della registrazione di protocollo. In questo senso, si può quindi affermare che il documento originale, nell'ambito del sistema documentale dell'Università, è quello registrato nel sistema del Protocollo Informatico.

I documenti informatici in ingresso oppure in uscita sono rispettivamente ricevuti e trasmessi in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'Amministrazione, oppure delle UOR/UU dell'Amministrazione.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che il destinatario del messaggio PEC ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma. Se il destinatario del messaggio PEC è un protocollista, procede in autonomia alla registrazione nel PdP; in caso contrario, invia una mail all'Ufficio Protocollo con allegato il messaggio ricevuto in formato "eml" e con il file primario allegato al messaggio PEC ricevuto. Nel testo della mail sono specificati, in tal caso, anche i metadati di registrazione: mittente, destinatario/i, oggetto e voce di classificazione. La registrazione di protocollo conterrà quindi come file primario il documento informatico sottoscritto con firma digitale e come allegato la busta di trasporto PEC completa.

Nel caso di documenti informatici in partenza, l'UOP oppure direttamente l'RPA se abilitato, effettua la registrazione di protocollo del documento informatico sottoscritto con firma digitale. Tale documento è inviato all'UOP mediante posta elettronica interna, all'indirizzo dell'Ufficio stesso preposto a questa funzione. Nel testo della mail sono specificati, in tal caso, anche i metadati di registrazione: mittente, destinatario/i, oggetto e voce di classificazione.

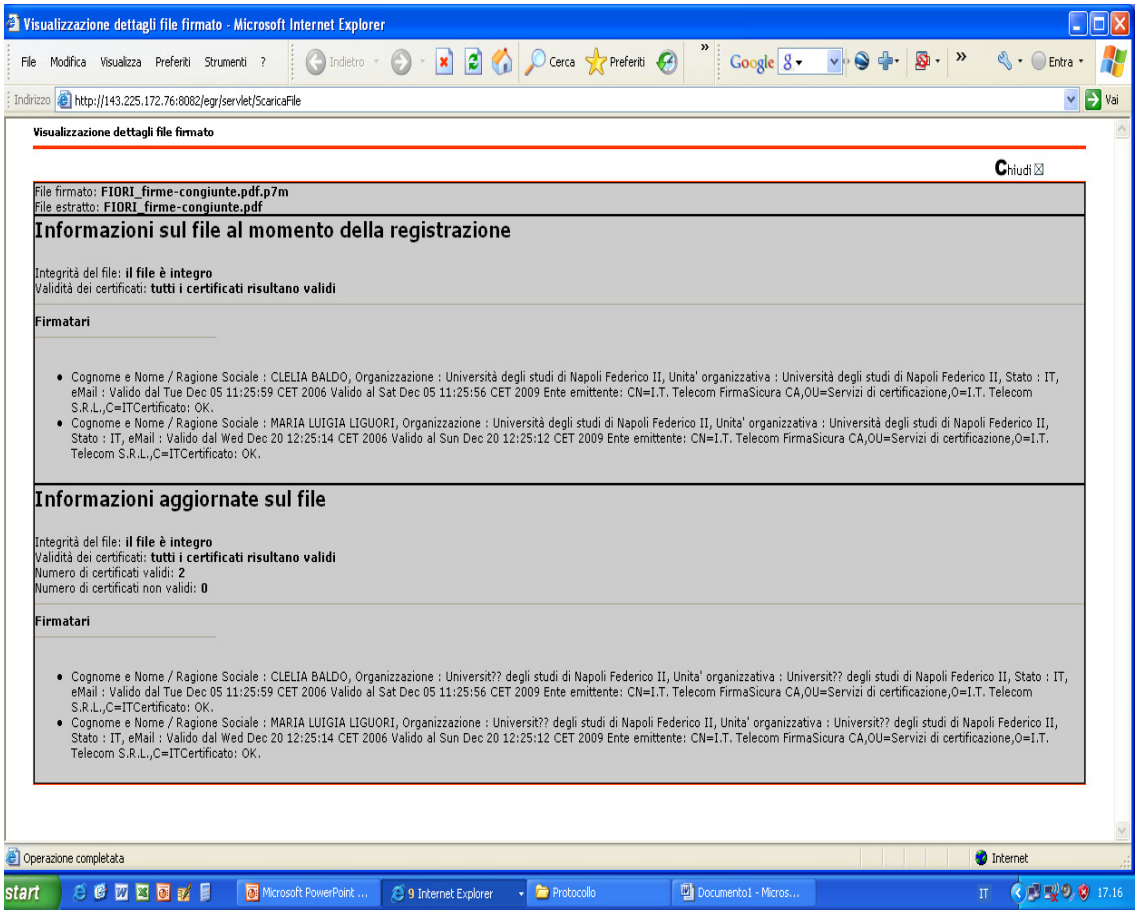
In tutti i casi, il PdP esegue una verifica di autenticità e integrità de documento: nel caso in cui il documento non sia integro, non ne è consentita la registrazione; se la verifica di autenticità fallisce (ad esempio, perché un certificato è scaduto), il sistema avvisa l'operatore che può decidere di interrompere l'operazione. Tali informazioni relative alla verifica di integrità ed autenticità del documento all'atto della protocollazione sono memorizzati in modo immodificabile. Il PdP esegue le stesse verifiche all'atto della consultazione della registrazione stessa, fornendo i dati alla data della verifica effettuata, come mostrato più avanti.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

Di seguito, si riportano le informazioni visualizzate dal Protocollo Informatico per ciascun documento firmato digitalmente e protocollato, relative allo stato e al

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

contenuto dei certificati di firma dei sottoscrittori sia al momento della visualizzazione che della registrazione di protocollo:



10.3.2. Documenti analogici (cartacei e supporti rimovibili)

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

La registrazione di protocollo di un documento analogico cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'Amministrazione ha la funzione di registrare l'avvenuta ricezione.
Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.4. Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, su richiesta del Responsabile UOR, l'UOP può modificare e integrare gli elementi facoltativi del protocollo.

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

I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche. I dati facoltativi sono ulteriormente distinti in "**Dati soggetti ad annullamento**" e "**Dati modificabili**".

Sono attributi del primo tipo:

- Oggetto;
- Mittente/destinatario;
- File primario e/o allegati;
- Estremi della Registrazione di emergenza.

La modifica a tali campi può essere completata da una nota con le motivazioni della modifica riportate dall'operatore dell'UOP, il cui profilo di abilitazione lo autorizza all'esecuzione della funzionalità di modifica dati di protocollazione.

Il PdP consente anche di modificare i dati "modificabili", in dettaglio:

- Tipo di documento;
- Mezzo di trasmissione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- Collegamento a documenti precedenti e susseguenti;
- Indicazione del livello di sicurezza (riservatezza) se diverso da quello standard applicato dal sistema di protocollazione;

Una funzione specifica consente di modificare inoltre i dati relativi alla classificazione e alla fascicolazione del documento.

10.5. Segnatura di protocollo dei documenti

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Essa consente di individuare ciascun documento in modo inequivocabile.

10.5.1. Documenti informatici

La soluzione generale

I dati della segnatura di protocollo di un documento informatico ricevuti da un sistema di protocollo interoperabile sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD).

Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'Amministrazione;
- data e numero di protocollo del documento.

È facoltativo riportare anche le seguenti informazioni:

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

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

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

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

Qualora l'Amministrazione decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal CNIPA (oggi Agenzia per l'Italia Digitale), includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

Come già detto in precedenza, il modulo interoperabilità, anche se presente nel PdP, alla data non è stato attivato. Di seguito le considerazioni che hanno motivato la decisione di posticipare l'avvio dell'utilizzo di tale modulo:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1. la scarsa diffusione ad oggi del meccanismo stesso tra le PPAA,
2. la necessità di essere interoperabili anche con privati e con cittadini,
3. le problematiche tecnico-organizzative che il suo utilizzo comporterebbe in una AOO con UOP distribuiti, come nel caso dell'amministrazione Federico II.

Tali motivazioni hanno indotto l'Amministrazione a pianificare l'avvio di tale funzionalità avanzata a sistema completamente avviato e maturo, comunque entro il 2013.

Di seguito, quindi, s'illustra la prassi attualmente seguita dall'Ateneo sia per lo scambio di documenti con altre PPAA che con cittadini e società esterne.

La soluzione dell'Università

Il problema principale che l'Amministrazione si è posta è, quindi, quello di fornire una rappresentazione del documento informatico originario (sottoscritto digitalmente) che sia completa di segnatura e in formato tale da risultare di semplice utilizzo mediante strumenti informatici largamente diffusi, fornendo anche l'evidenza dei nominativi dei sottoscrittori, in modo da assicurare l'integrità di tale riproduzione.

La soluzione adottata dall'Università degli Studi di Napoli per rispondere alle esigenze sopra riportate è l'utilizzo del Timbro digitale, soluzione coerente con le indicazioni riportate nella Circolare n. 62/2013 redatta dall'Agenzia per l'Italia Digitale relativa alle "Linee guida per il contrassegno generato elettronicamente" e da questa approvata. La soluzione consiste nell'apposizione su ciascuna pagina (o selezione di pagine) del documento originale – a richiesta dell'utente del Protocollo Informatico – dei dati salienti di registrazione di protocollo: codice, data e ora di registrazione, denominazione AOO e UOR di protocollazione e elenco dei nominativi dei firmatati, nonché di un codice crittografico bidimensionale. Tale contrassegno contiene gli stessi dati riportati nella segnatura in chiaro, con l'aggiunta dell'impronta elettronica del documento (impronta associata, in maniera immodificabile, al documento nel sistema del Protocollo Informatico). Il documento originale viene quindi rappresentato in un nuovo documento "pdf", esportabile e stampabile in modo molto semplice.

Per la decodifica delle informazioni contenute nel timbro digitale apposto sui documenti protocollati, è disponibile sul sito Praxis la versione del software open source "BC Tester" che può essere scaricato dall'utente con poche semplici operazioni.

In **allegato 14**, si riportano alcune informazioni di carattere generale sui contrassegni elettronici, anche denominati timbri digitali.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.5.2. Documenti cartacei

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

- denominazione dell'Amministrazione;
- denominazione della UOR che ha eseguito la registrazione;
- data (facoltativamente, ora) e numero di protocollo del documento.

Nel caso dell'Amministrazione Centrale, la segnatura dei documenti protocollati dall'UOP avviene contestualmente alla acquisizione dell'immagine del documento, in fase di scansione. Per i documenti in partenza, tale segnatura è orizzontale in alto; per quelli in arrivo è verticale a destra.

Nel caso delle restanti UOR, il "segno" grafico è realizzato con una etichetta autoadesiva corredata di codice a barre. L'operazione di acquisizione dell'immagine dei documenti cartacei è in tal caso eseguibile solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

L'Amministrazione ha optato per il "segno" riportato nell'**allegato 14**.

Il "segno" della segnatura di protocollo deve essere apposto sulla prima pagina dell'originale.

10.6. Annullamento delle registrazioni di protocollo

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

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

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

Per ogni operazione di annullamento il sistema, al fine di adeguarsi al dettato normativo, richiede un provvedimento di autorizzazione. Pertanto, nel caso in cui si ravvisi la necessità di annullare una o più registrazioni di protocollo (per esempio

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

perché si tratta di una duplicazione di registrazione), il responsabile della struttura (UOR/UO) o, nel caso dell'Amministrazione centrale, il Responsabile del servizio di protocollo informatico (a seguito di richiesta scritta trasmessa anche via fax o e-mail indicante il numero di protocollo da annullare e i motivi dell'annullamento) dovrà autorizzare l'annullamento con apposito atto sottoscritto. Il protocollista, a valle del processo di autorizzazione, provvederà a protocollare l'atto, immettendo in fase di registrazione, le seguenti informazioni:

1. nel campo mittente e destinatario, la propria UOR/UO;
2. nel campo oggetto, l'oggetto della nota di annullamento, con il numero di protocollo (PG) da annullare;
3. nel campo note (facoltativamente) la motivazione dell'annullamento

Tale operazione è da svolgersi preliminarmente all'avvio della procedura di annullamento che è costituita dalle tre fasi di seguito riportate:

A. inserimento del l'atto precedentemente protocollato nell'elenco degli atti di autorizzazione all'annullamento,
B. associazione dell'atto di autorizzazione alla registrazione di protocollo da annullare: quest' ultima assume lo stato di "annullabile",
C. annullamento vero e proprio della registrazione di protocollo.

Le operazioni precedentemente elencate sono dettagliatamente illustrate nel "Manuale Operativo del Protocollo" disponibile sul sito dell'eGovernment Praxis.

10.7. Livello di riservatezza

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema. Lo strumento attraverso il quale è possibile garantire la riservatezza dei documenti (in forma più leggera rispetto al protocollo Particolare) è rappresentato dalle Access Control List, tramite le quali è possibile impostare, per ogni singolo documento e in forma sempre modificabile, i permessi di accesso e visibilità, come meglio descritto nel capitolo dedicato alla sicurezza del PdP.

Inoltre, il sistema consente di definire un attributo specifico di "Riservato" per ciascun documento. In tal caso, il documento risulterà visibile solo dagli utenti del PdP abilitati all'accesso e inoltre dotati dell'abilitazione specifica alla consultazione dei documenti "Riservati".

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.8. Casi particolari di registrazioni di protocollo

10.8.1. Registrazioni di protocollo particolari

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione un registro di protocollo particolare, non disponibile alla consultazione dei soggetti non espressamente abilitati, funzionalità già ampiamente descritta nel precedente capitolo 8. Tale registro contiene:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente richiamati nell'allegato 11.

Nel caso di registrazione nel protocollo particolare è necessario indicare, contestualmente alla registrazione, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

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

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

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

10.8.2. Circolari e disposizioni generali

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.8.3. Documenti cartacei in partenza con più destinatari

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

Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

10.8.4. Documenti cartacei ricevuti a mezzo telegramma

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

10.8.5. Documenti cartacei ricevuti a mezzo telefax

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

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

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

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

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

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

Il documento in partenza reca una delle seguenti diciture:

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

La segnatura viene apposta sul documento e non sulla copertina di trasmissione.

La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche.

In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

10.8.6. Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione all'UOP preventiva, onde concordare tempi e modi di protocollazione e di spedizione.

10.8.7. Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.

Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, essi saranno accantonati e protocollati successivamente, così come descritto più avanti, nell'ambito della procedura di protocollazione differita. In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta, senza gli estremi del protocollo.

10.8.8. Fatture, assegni e altri valori di debito o credito

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall'altra posta in arrivo e inviate quotidianamente alla UOR competente che provvede alla loro registrazione su un repertorio dedicato diverso da quello generale.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.8.9. Protocollazione di documenti inerenti a gare di appalto confezionate su supporti cartacei

La corrispondenza dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, a un concorso o simili non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura di protocollo direttamente sulla busta, plico o simili. Nel caso la consegna del plico sia effettuata all'UOP entro la data e ora prevista dal bando ma per motivi organizzativi legati alla coda alla sportello di registrazione sia superata l'ora limite prevista, può essere seguita la procedura di protocollazione differita precedentemente descritta.

Tutta la corrispondenza relativa a ciascuna gara verrà trasmessa a cura dell'UOP con apposita lettera di accompagnamento, debitamente protocollata, all'UOR/UU competente.

È compito dello stesso UOR/UU provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

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

Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il Responsabile del Servizio/Ufficio Protocollo dell'Amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

10.8.10. Protocolli urgenti

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

Solo in questo caso il Responsabile UOP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da spedire.

Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'UOP.

10.8.11. Documenti non firmati

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali. È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

10.8.12. Protocollazione dei messaggi di posta elettronica convenzionale

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

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

10.8.13. Protocollo di documenti digitali pervenuti erroneamente

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

10.8.14. Ricezione di documenti cartacei pervenuti erroneamente

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

10.8.15. Copie per conoscenza

Nel caso di copie per conoscenza con più destinatari per conoscenza, si deve utilizzare la procedura descritta nel paragrafo 10.8.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza, valorizzando l'opportuno indicatore nella maschera di registrazione.

10.8.16. Differimento delle registrazioni

Nel caso di un temporaneo ed eccezionale carico di lavoro che non permetta di evadere la corrispondenza ricevuta nella medesima giornata lavorativa o comunque entro 24 ore dal ricevimento e qualora dalla mancata registrazione di protocollo del documento

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di offerte ad un bando di gara in scadenza), è autorizzato, con motivato provvedimento del Responsabile UOR (oppure, dell' UOP), l'uso del protocollo differito.

Il protocollo differito consiste nel differimento della decorrenza giuridica dei termini di arrivo del documento rispetto alla data di registrazione, dichiarandone espressamente la data effettiva di arrivo, le motivazioni del ritardo e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

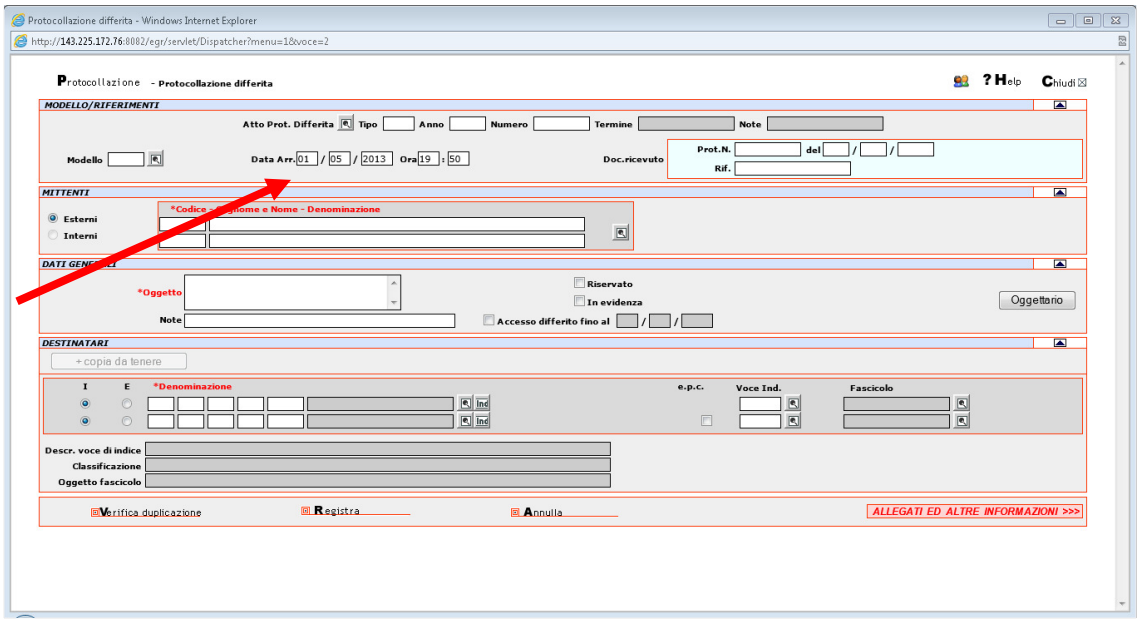
Il ricorso al protocollo differito si applica solo ai documenti in arrivo ed è autorizzato dal responsabile UOR (oppure, dell'UOP), anche su motivata richiesta dell'RPA, mediante la sottoscrizione di un provvedimento di autorizzazione in cui si riportano le motivazioni del differimento, la data e ora di effettivo arrivo dei documenti, il numero e la descrizione dei documenti e la data entro la quale sarà eseguita.

Agli interessati, se necessario, viene dunque resa nell'immediato una ricevuta di consegna priva del codice di protocollo.

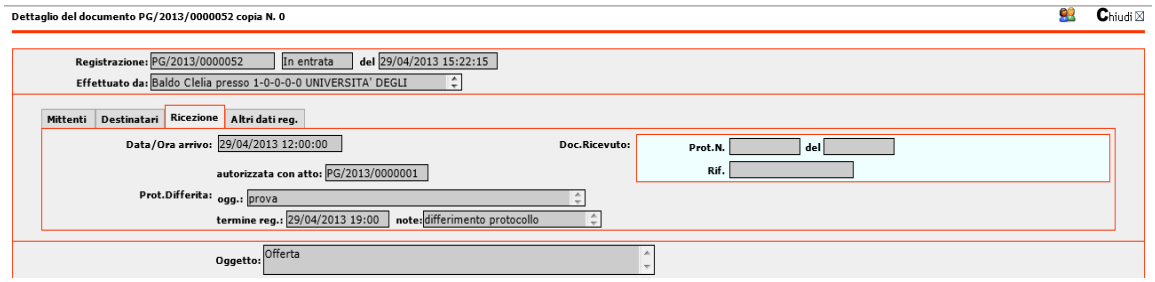
In pratica il responsabile UOR (oppure, dell'UOP), dopo aver assunto il provvedimento di differire le operazioni di registrazione ed averlo registrato nel sistema di protocollo quale atto autorizzativo di differimento, provvede a chiudere in un plico o in un armadio chiuso a chiave o in una stanza chiusa a chiave i documenti da protocollare.

All'atto della registrazione dei documenti di cui è stata autorizzato il differimento della protocollazione, l'operatore di protocollo valorizza quindi il campo "data e ora arrivo", come di seguito riportato e collegherà inoltre ciascuna registrazione differita al codice di protocollo del provvedimento di differimento sottoscritto dal responsabile UOR/UOP.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



A conclusione delle operazioni di registrazione, il documento protocollato è collegato in modo indissolubile al provvedimento di autorizzazione. Nei dettagli sarà anche mostrata l'ora di effettivo arrivo del documento, attestata anche dal provvedimento di autorizzazione, come mostrato di seguito:



10.8.17. Registrazioni di documenti temporaneamente riservati

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

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

10.8.18. Corrispondenza personale o riservata

La corrispondenza sulla cui busta è riportato il nominativo del destinatario è regolarmente aperta dagli uffici incaricati della sigla ed assegnazione della

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

corrispondenza in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".

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

10.8.19. Integrazioni documentarie

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

Tale verifica spetta al responsabile del procedimento amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento. I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

10.9. Gestione delle registrazioni di protocollo con il PdP

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

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

10.10. Registrazioni di protocollo

10.10.1. Attribuzione del protocollo

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

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

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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

10.10.2. Registro informatico di protocollo

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

1. estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di protocollo;
2. applicazione di un riferimento temporale al file così prodotto mediante registrazione dello stesso nel PdP;
3. salvataggio, per anno solare, dei file a partire dal sistema di esercizio del PdP a cura di RSP e creazione di pacchetti di versamento;
4. conservazione[6] di tali pacchetti a cura del Responsabile della Conservazione.

Con particolare riguardo ai punti 1, 2 e 3, viene eseguita la seguente procedura automatizzata: ogni giorno viene eseguito in automatico il processo di estrazione del file Pdf contenente gli estremi delle registrazioni di protocollo eseguite nella giornata.Il file viene archiviato nella cartella del file system: /allegati/stampe/reportGiornalieri. La denominazione del file conterrà la data di riferimento del report, nel formato gg-mm-AAAA. Per garantire la non modificabilità delle informazioni contenute nel file, il registro è quindi protocollato in automatico nel sistema del PdP. L'oggetto della registrazione è "Stampa del registro di protocollo del gg/mm/AAAA", il mittente ed il destinatario coincidono e sono la AOO stessa, i documenti sono collocati nel fascicolo 2009/I.007/8. Tali registrazioni di protocollo sono quindi accessibili solo all'RSP e alle postazioni di amministrazione presso RSI.

È a carico del RSI archiviare in modalità sicura le copie dei registri giornalieri di protocollo.

In fase di conservazione la disponibilità e l'integrità degli stessi, a partire dal pacchetto di versamento prodotto da RSP e da questi consegnato al sistema di conservazione, sarà garantita dal Responsabile della Conservazione.

L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo[7].

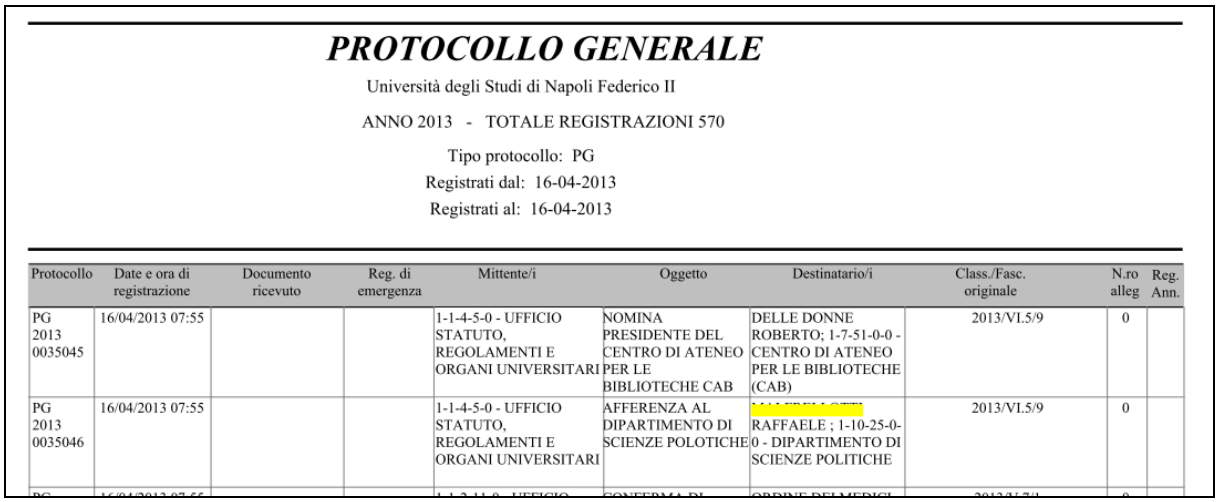
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.

Di seguito, si riporta l'esempio del layout di stampa:

6 A valle dell'avvio del Servizio di Conservazione.

7 Le copie giornaliere generali di back-up dell'intero sistema informativo dell'Amministrazione esulano dai meccanismi di sicurezza qui richiamati

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



PROTOCOLLO GENERALE

Università degli Studi di Napoli Federico II

ANNO 2013 - TOTALE REGISTRAZIONI 570

Tipo protocollo: PG
Registrati dal: 16-04-2013
Registrati al: 16-04-2013

Protocollo	Date e ora di registrazione	Documento ricevuto	Reg. di emergenza	Mittente/i	Oggetto	Destinatario/i	Class./Fasc. originale	N.ro alleg	Reg. Ann.
PG 2013 0035045	16/04/2013 07:55			1-1-4-5-0 - UFFICIO STATUTO, REGOLAMENTI E ORGANI UNIVERSITARI	NOMINA PRESIDENTE DEL CENTRO DI ATENEO PER LE BIBLIOTECHE CAB	DELLE DONNE ROBERTO; 1-7-51-0-0 - CENTRO DI ATENEO PER LE BIBLIOTECHE (CAB)	2013/VI.5/9	0	
PG 2013 0035046	16/04/2013 07:55			1-1-4-5-0 - UFFICIO STATUTO, REGOLAMENTI E ORGANI UNIVERSITARI	AFFERENZA AL DIPARTIMENTO DI SCIENZE POLOTICHE	[redacted] RAFFAELE ; 1-10-25-0-0 - DIPARTIMENTO DI SCIENZE POLITICHE	2013/VI.5/9	0	

10.10.3. Tenuta delle copie del registro di protocollo

I dati contenuti nei pacchetti di versamento sono conservati con le modalità previste dalla normativa vigente e dal Manuale di Conservazione adottato dall'Amministrazione.

Nelle more dell'avvio del sistema di conservazione, con frequenza annuale, RSP provvede al salvataggio (in duplice copia) dei file su CD e consegna degli stessi in busta chiusa a RSI affinché siano custoditi nell'armadio ignifugo presso il CED del Centro Storico.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

11. DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'Amministrazione con particolare riferimento alle modalità di utilizzo dello stesso. Si tratta di una descrizione completa anche se sintetica che tuttavia non tratta delle modalità operative perché le stesse sono trattate dettagliatamente nei manuali operativi utente del PdP.

I manuali operativi utente sono allegati esterni al presente manuale e sono comunque consultabili on-line sulla intranet dell'Amministrazione, in particolare, nella sezione Protocollo Informatico disponibile all'indirizzo del sito Praxis dedicato alle iniziative per l'eGovernment di Ateneo.

11.1. Descrizione funzionale ed operativa

11.1.1. La soluzione adottata dall'Università

Dal punto di vista tecnico, dopo una fase di ricognizione e di valutazione di alcune proposte di mercato, l'Università ha individuato come applicativo più rispondente alle proprie esigenze il prodotto E-Grammata realizzato dalla società Engineering S.p.A., per conto della Regione Campania. In linea con quanto disposto dalla normativa vigente per quanto riguarda il miglioramento dell'efficienza operativa della pubblica amministrazione e di contenimento della spesa pubblica (ai sensi degli artt.1 e 2 del DPCM "Razionalizzazione in merito all'uso delle applicazioni informatiche e servizi ex articolo 1, commi 192, 193 e 194 della legge n. 311 del 2004 (Finanziaria 2005)" del 31.5.05), nonché con il Capo VI del Codice dell'Amministrazione Digitale, rubricato "Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni", l'Ateneo ha quindi richiesto ed ottenuto dalla Regione Campania, tramite la stipula di una convenzione, il riuso di tale applicazione di Protocollo Informatico.

11.1.2. Le funzionalità dell'applicazione E-Grammata

Le funzionalità del sistema sono descritte nel "Manuale utente E-Grammata" e nella "Guida all'utilizzo del Protocollo Informatico dell'Università" disponibili all'indirizzo www.praxis.unina.it/protocollo.

Nei paragrafi successivi sono comunque riportate le principali funzionalità ad oggi disponibili nel sistema.

11.1.2.1 Le funzionalità generali

Il sistema implementato offre le seguenti macro- funzionalità:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Nucleo minimo di protocollo: registrazione, segnatura e classificazione dei documenti in ingresso ed in uscita dall'Ateneo oppure interni;
Gestione informatica dei documenti: acquisizione ottica dei documenti, versionamento, assegnazione, fascicolazione, conservazione, workflow dell'iter amministrativo interno;
Gestione dei profili di autorizzazione degli utenti per l'utilizzo di funzioni e per l'accesso ai dati;
Interoperabilità avanzata con Enti esterni mediante l'utilizzo di strumenti di PEC (Posta Elettronica Certificata), di Firma Digitale e di segnatura informatica dei documenti.

In aggiunta, il sistema implementato presso l'Ateneo offre le seguenti funzionalità aggiuntive rispetto all'installazione "base" di E-Grammata:

- Gestione della Pianta organica, dell'anagrafica e dei gruppi
- Fascicolazione automatica
- Stampa automatica in forma immodificabile del registro di protocollo
- Stampa della etichetta consentita solo alla UOR protocollante
- Gestione modifiche registrazione/annullamento per UOR protocollante
- Autenticazione mediante LDAP mediante Webservice UNINA e servizi di sicurezza e abilitazione, per riconoscere gli utenti e concedere l'accesso ai documenti e alle funzioni di competenza di ciascuno, comprendendo le funzioni per la definizione e la gestione della struttura organizzativa dell'Ente
- Storicizzazione allegati
- Ricerca avanzata
- Miglioramento della gestione "lista lavoro", soprattutto riguardo alle "copie conoscenza"
- Ricerca dei documenti per ottenere la UO protocollante
- Segnalazione file mancante in lista lavoro
- Firma digitale: memorizzazione esito verifica integrità e autenticità, gestione firmatari multipli, apposizione timbro crittografico con segnatura di protocollo sulla riproduzione pdf del documento
- Miglioramento dei meccanismi di sicurezza connessi alla gestione del flusso documentale
- Client di emergenza
- Memorizzazione immagini su SAN
- Utilizzo Log4J
- Gestione delle code di stampa
- Adeguamento (parziale) per accessibilità
- Ricerca avanzata dei documenti registrati
- Integrazione con il sistema di autenticazione (IAM)
- Integrazione con il sistema di firma centralizzata
- Gestione dell'iter di approvazione ed emanazione decreti ed ordini di servizio

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Gestione della produzione in modalità automatizzata delle copie conformi

Più in dettaglio, di seguito, la griglia di corrispondenza delle funzionalità offerte dal sistema E-Grammata con la normativa vigente[8] da cui si deduce l'adeguatezza del sistema di alla normativa vigente in materia di protocollo informatico e gestione dei flussi documentali:

11.1.2.2 Le funzionalità di gestione dati di profilazione

Riferimento Normativo	Descrizione
[TU4452000/52/1/a]	Garanzie di sicurezza e integrità del sistema
[DPCM311000/7/1]	Requisiti minimi di sicurezza del sistema operativo dell'elaboratore
[DPCM311000/7/2] [TU445/52/1e]	Disponibilità di meccanismi che consentano il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti in condizioni di sicurezza nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
[DPCM311000/7/3]	Tracciamento da parte del sistema di protocollo informatico di qualsiasi evento di modifica delle informazioni trattate e individuazione del suo autore
[DPCM311000/7/4]	Protezione delle registrazioni di tracciamento da modifiche non autorizzate
[TU4452000/52/1/b]	Garanzie sulla corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita
[TU4452000/53/1/a]	Generazione automatica del numero di protocollo e sua registrazione in forma non modificabile
[TU4452000/57/1]	Il numero di protocollo è un numero progressivo e costituito da almeno sette cifre numeriche e la numerazione di protocollo è rinnovata ogni anno solare
[TU4452000/53/1/b]	Generazione automatica della data di registrazione di protocollo e sua registrazione in forma non modificabile
[TU4452000/53/1/c]	Registrazione in forma non modificabile del mittente per i documenti ricevuti o, in alternativa, del destinatario o dei destinatari per i documenti spediti
[TU4452000/53/1/d]	Registrazione in forma non modificabile dell'oggetto del documento
[TU4452000/53/1/e]	Possibilità di registrare la data e protocollo del documento ricevuto, se disponibili
[TU4452000/53/1/f]	Registrazione in forma non modificabile dell'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto

[8] Nella tabella con TU4452000 si fa riferimento al DPR 445/2000.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Riferimento Normativo	Descrizione
[DPCM311000/17/2]	L'impronta è generata utilizzando la funzione di hash, definita nella norma ISO/IEC 10118-3:1998, Dedicated Hash-Function 3, corrispondente alla funzione SHA-1
[TU4452000/53/3]	Assegnazione delle informazioni nelle operazioni di registrazione di protocollo effettuata dal sistema in un'unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati
[TU4452000/54/1] [DPCM311000/8]	Esistenza di una funzione di annullamento delle informazioni non modificabili delle registrazioni e/o dell'intera registrazione
[TU4452000/54/1] [DPCM311000/8]	Memorizzazione delle informazioni annullate nella base di dati
[TU4452000/54/2]	Mantenimento per le informazioni annullate di una dicitura o un segno in posizione sempre visibile e tale da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione
[TU4452000/55/1]	Apposizione in forma permanente e non modificabile della segnatura di protocollo all'originale del documento
[TU4452000/55/1] [DPCM311000/9/1]	Presenza nella segnatura di protocollo delle informazioni minime per l'identificazione univoca di ciascun documento: codice identificativo dell'Amministrazione, codice identificativo dell'Area Organizzativa Omogenea, progressivo di protocollo, data di protocollo
[TU4452000/55/2]	L'operazione di segnatura del protocollo effettuata contemporaneamente all'operazione di registrazione di protocollo
[TU4452000/55/3]	La segnatura di protocollo può includere ulteriori informazioni quali il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo
[TU4452000/53/2]	Produzione del registro giornaliero di protocollo
[TU4452000/63/5]	Esistenza di un'apposita funzione di recupero dei dati che consenta l'inserimento delle informazioni relative ai documenti protocollati in emergenza, in seguito ad interruzione nella disponibilità della procedura informatica, senza ritardo al ripristino delle funzionalità del sistema
[TU4452000/63/5]	Attribuzione durante la fase di ripristino a ciascun documento registrato in emergenza di un numero di protocollo del sistema informatico ordinario

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Riferimento Normativo	Descrizione
[TU4452000/63/5]	Correlazione stabile tra il numero di protocollo del sistema informatico ordinario con il numero utilizzato in emergenza
[TU4452000/52/1/c]	Fornitura da parte del sistema delle informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali
[TU4452000/52/1/f]	Disponibilità di funzioni per il supporto e la gestione del sistema di classificazione d'archivio (titolario d'archivio)
[*derivato*]	Funzioni che consentano l'utilizzo di strumenti di navigazione grafica e di browsing all'interno del sistema di classificazione adottato (a fini di selezione, ricerca, visualizzazione)
[TU4452000/52/1/f]	Corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato
[*derivato*]	Funzione di numerazione progressiva automatica dei fascicoli
[*derivato*]	Funzioni di gestione dei fascicoli
[*derivato*]	Funzioni per la creazione, la gestione e la manutenzione dell'organigramma dell'amministrazione
[*derivato*]	Il sistema deve gestire un indice dei corrispondenti in modo da facilitare le operazioni di protocollazione dei documenti ricevuti e spediti. Deve essere possibile effettuare delle ricerche ed alimentare l'indice attraverso le operazioni di protocollazione
[TU4452000/52/1/d]	Reperimento delle informazioni riguardanti i documenti registrati
[TU4452000/58/2]	Esistenza di criteri di selezione basati su tutti i tipi di informazioni registrate per la ricerca delle informazioni del sistema
[TU4452000/58/3]	Possibilità di elaborazioni statistiche sulle informazioni registrate

11.1.2.3 Le funzionalità di sicurezza

Riferimento Normativo	Descrizione
[TU4452000/61/3/a]	Attribuzione del livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento ed alla modifica delle informazioni
[TU4452000/63/1]	Procedura di registrazione in emergenza
[TU4452000/63/3]	Scrittura del numero totale di operazioni registrate manualmente per ogni giornata di registrazione in emergenza sul registro di emergenza
[TU4452000/63/4]	Garanzia dell'identificazione univoca dei documenti registrati

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Riferimento Normativo	Descrizione
	nell'ambito del sistema documentario dell'area organizzativa omogenea consentita dalla sequenza numerica utilizzata su un registro di emergenza
[DPCM311000/7/5]	Riversamento su supporti informatici non riscrivibili, almeno al termine della giornata lavorativa, del contenuto del registro informatico di protocollo

11.1.2.4 Le funzionalità per la gestione documentale

Riferimento Normativo	Descrizione
[*derivato*]	Acquisizione dei documenti cartacei in formato immagine attraverso uno scanner
[*derivato*]	Acquisizione di documenti da file system
[*derivato*]	Acquisizione documenti da casella di posta elettronica
[*derivato*]	Gestione dei principali formati dei documenti elettronici
[*derivato*]	Immodificabilità dei documenti acquisiti nel sistema e protocollati
[*derivato*]	Visualizzazione e stampa dei documenti
[*derivato*]	Funzionalità di OCR ausiliari alle operazioni di Protocollazione
[*derivato*]	Funzionalità di OCR per consentire ricerche full text sui documenti acquisiti in formato immagine
[*derivato*]	Ricerche full text estese al contenuto del documento informatico
[*derivato*]	Trasparenza dei sistemi hardware di memorizzazione in modalità "on-line", "near-line" ed "off line"

11.1.2.5 Le funzionalità per la gestione del lavoro cooperativo ed interoperabilità

Riferimento Normativo	Descrizione
[*derivato*]	Il sistema deve prevedere la definizione e la gestione di Access Control List (ACL) sui documenti e sui fascicoli
[*derivato*]	Gestione di meccanismi di visibilità dei documenti sulla base della posizione gerarchica degli utenti e dei ruoli
[*derivato*]	Invio di notifiche per gli eventi più significativi che accadono all'interno del sistema
[*derivato*]	Gestione dell'archivio corrente

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

[TU4452000/67/1]	Gestione dell'archivio di deposito
[TU4452000/65/1/a]	Correlazione dei fascicoli ai procedimenti amministrativi
[*derivato*]	Integrazione con motori di Workflow
[DPCM311000/15/1] [TU4452000/14/1]	Lo scambio dei documenti informatici soggetti alla registrazione di protocollo è effettuato mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni
[DPCM311000/15/2]	Corrispondenza di una unica operazione di registrazione di protocollo ad ogni messaggio di posta elettronica ricevuto da una area organizzativa omogenea
[DPCM311000/18/1]	I dati relativi alla segnatura di protocollo di un documento trasmesso da una area organizzativa omogenea sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML) 1.0 (raccomandazione W3C 10 febbraio 1998), conforme con un file DTD (Document Type Definition) di cui alla circolare Aipa n. 28 del 7/5/2001, ovvero alla sua versione più recente
[DPCM311000/19/1] [DPCM311000/19/2]	Requisito di completezza della segnatura informatica
[AIPACIRC28/5]	Il sistema deve trattare messaggi protocollati codificati secondo una struttura MIME, forma di codifica che rappresenta la modalità di aggregazione di documenti informatici ai fini della trasmissione in un unico messaggio
[AIPACIRC28/5]	La segnatura informatica è contenuta in una body part avente nome Segnatura.xml. L'uso del nome Segnatura.xml per una body part è riservato a questo unico scopo
[DPCM311000/18/ 3]	Il sistema deve supportare e/o integrare strumenti di firma elettronica ai fini della sottoscrizione dei documenti informatici e alla loro gestione (visualizzazione, verifica della firma)
[AIPACIRC28/6]	Gestione automatica dei messaggi di ritorno
[AIPACIRC28/6/1]	Gestione messaggi di conferma di ricezione
[AIPACIRC28/6/2]	Gestione messaggi di notifica di eccezione
[AIPACIRC28/6/3]	Gestione messaggi di aggiornamento di conferma
[AIPACIRC28/6/4]	Gestione messaggi di annullamento di protocollazione
[DPCM311000/17/1]	Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici va calcolata per tutti i file inclusi nel messaggio di posta elettronica l'impronta di cui all'art. 53, comma 1, lettera f), del Testo unico n. 445/2000
[DPCM311000/11]	Il sistema dovrà prevedere delle funzioni di accesso all'Indice delle Amministrazioni pubbliche e delle Aree organizzative omogenee

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

11.1.2.6 Stampe e demone di stampa

E-Grammata prevede diverse funzionalità di stampa in due modalità: al volo o schedulati in un demone qualora le dimensioni dell'output superino un margine precedentemente stabilito, configurabile.

Anche in questo caso, un ulteriore parametro di sistema determina l'area di memoria fisica dove vengono riversate le stampe generate dall'applicativo o dal demone di stampa. A conclusione del processo di stampa, tale area viene cancellata.

11.1.2.7 Le funzioni crittografiche

Il PdP dispone di un insieme di librerie e di funzioni crittografiche, con lo scopo di consentire la completa gestione dei documenti digitali: dalla formazione, alla registrazione di protocollo, alla verifica e riproduzione a norma.

Appartengono al sistema un archivio sicuro di certificati, CertStore, che consente la gestione dei certificati emessi dalle Certification Authority ed il servizio che permette di scaricare le CRL (gli elenchi contenenti i certificati revocati) aggiornate.

È in corso attualmente l'integrazione del PdP con il servizio centralizzato di Firma digitale dell'Università denominato Confirma.

11.2. L'architettura applicativa

Il protocollo si basa su un modello three-tier, i cui livelli sono:

- Tabelle e stored procedure su database Oracle
- Logica di controllo implementata da servlet su application server Tomcat
- Logica di visualizzazione dati, implementata da Java Server Pages, codice Javascript e applet

La logica business è realizzata tramite stored procedure, che vengono invocate in corrispondenza di una richiesta http del browser.

La logica di controllo è sostanzialmente realizzata mediante un componente (una Servlet) che riceve le richieste http, esegue le chiamate alle stored procedure su database e infine invia il controllo alla parte di presentazione (Java Server Pages) dei dati.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

11.3. L'acquisizione massiva dei documenti analogici

La soluzione implementata, per quanto riguarda l'Amministrazione Centrale dove la mole di documenti da protocollare è spesso rilevante, con frequenti situazioni critiche di picco prevede l'utilizzo di scanner massivi che consentono di apporre la segnatura di protocollo e l'acquisizione delle immagini in modo integrato con la funzionalità di completamento dei metadati di registrazione. Il processo è descritto dalla sequenza seguente:

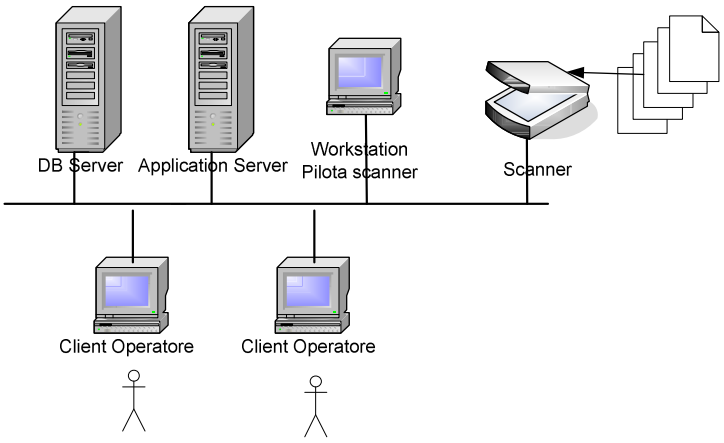
1. I documenti sono organizzati in lotti di lavorazione. Un lotto è un insieme di documenti di caratteristiche simili o per numerosità dei fogli che costituiscono ciascun documento, oppure per analogia di oggetto/procedimento amministrativo a cui i documenti si riferiscono.
2. Nell'ambito di un lotto, i documenti sono separati mediante un foglio separatore, identificato dalla presenza di un particolare codice a barre che viene letto e decodificato dallo scanner in fase di acquisizione delle immagini dei documenti che costituiscono un dato lotto. Per alcune lavorazioni (ad esempio quelle a foglio singolo), il foglio separatore su cui si trova il codice della lavorazione è posto solo all'inizio del lotto.
3. I lotti di documenti sono caricati nell'alimentatore automatico dello scanner.
4. Per ciascun documento da protocollare, viene eseguito, in logica transazionale, un processo automatico che:
    a. Acquisisce dal sistema il numero progressivo di protocollo,
    b. Invia allo scanner il numero progressivo di protocollo,
    c. Lancia il comando di segnatura del documento e di acquisizione dell'immagine del documento stesso e controlla l'esito dell'operazione;
    d. Calcola l'impronta (l'hash) dell'immagine, collegandola in modo indissolubile all'immagine del documento a cui si riferisce;
    e. Cataloga ed organizza le immagini acquisite, con i relativi codici hash, in code di lavorazione.
5. Gli operatori, a partire dalle immagini acquisite, accedono ad una apposita funzionalità del PdP per il completamento (oppure, il recupero, nel caso di errori) dei lotti. Il completamento (oppure, il recupero consiste nell'inserimento delle informazioni minime nel registro di protocollo (metadati). Tali operazioni si concludono entro poche ore dall'acquisizione ottica e, comunque, di regola entro la stessa giornata lavorativa.
6. Il sistema è ulteriormente irrobustito con ulteriori controlli applicativi eseguiti dal PdP che, a valle dell'invio dal client che pilota lo scanner al server, sono effettuati allo scopo di rilevare inconsistenze tra il numero di documenti pervenuti ed il numero atteso di protocolli per quel dato lotto. In condizioni di errore, il lotto viene posto in uno stato da "recuperare": le successive operazioni di controllo e correzione devono essere svolte prioritariamente da UoP dell'Amministrazione Centrale, entro la stessa giornata lavorativa.
7. In ogni caso, qualsiasi registrazione di protocollo priva di impronta e di metadati associati viene annullata dopo le ore 24 da un processo automatico.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Il colloquio con gli scanner è garantito da un software client denominato "Opus" che consente, in base alla tipologia di lotto, di gestire in modo opportuno la lavorazione del lotto da parte dello scanner. Le tipologie di lotti lavorati dagli scanner massivi sono di seguito riportate:

LAVORAZIONE	DESCRIZIONE
ARRIVO	Separatore di minuta + fogli(acquisisce tutte le immagini Fronte/Retro), timbra solo il primo foglio
ARRIVO_ALL *(nuova)*	Separatore di minuta + fogli(acquisisce tutte le immagini Fronte/Retro), timbra tutti i fogli
ARRIVO_S	Senza separatore di minuta, ad ogni foglio incrementa il numero(acquisisce tutte le immagini Fronte/Retro), timbra tutti i fogli
PARTENZA	Separatore di minuta + fogli[*separatore di documento + fogli, separatore di prima copia + fogli, separatore di allegati + fogli*], acquisisce tutti i fogli Fronte/Retro dietro il separatore minuta e dietro il separatore allegati, timbra il primo foglio dietro ogni separatore
PARTENZA_M	Separatore di minuta + fogli(ad ogni separatore incrementa il numero), acquisisce solo il primo foglio Fronte/Retro
PARTENZA_S	Incrementa il numero ogni due fogli e acquisisce solo il primo foglio Fronte/Retro, timbra tutti i fogli
PARTENZA_S1 *(nuova)*	Senza separatore di minuta, ad ogni foglio incrementa il numero(acquisisce tutte le immagini Fronte/Retro), timbra tutti i fogli
PARTENZA_S2	Incrementa il numero ogni tre fogli e acquisisce solo il primo foglio Fronte/Retro, timbra tutti i fogli

Di seguito, lo schema dell'architettura del sistema di acquisizione da scanner massivo.



Più dettagliatamente, dal punto di vista dell'architettura software, la Workstation che pilota lo scanner ospita il componente applicativo che gestisce, in modo sicuro:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1. la sincronizzazione con il sistema di protocollo,
2. la lettura dei lotti di documenti caricati nell'alimentatore dello scanner, la loro segnatura ed acquisizione dell'immagine,
3. il calcolo e l'associazione del codice hash all'immagine di ciascun documento,
4. la copia su file system del DB Server dei documenti acquisiti, il calcolo e l'associazione del codice hash all'immagine di ciascun documento.

Di seguito, le caratteristiche tecniche degli scanner utilizzati per la segnatura massiva presso l'Ufficio di Protocollo dell'Amministrazione Centrale.

Scanner Kodak 1840 / i610/ DS 5500 D	
Tipo:	rotativo versione *double-side* per la scansione del fronte e del retro del foglio in una sola operazione
Formato carta:	fino a A3 in verticale e orizzontale
Alimentazione fogli:	sia manuale che automatica mediante cassetto di 350 fogli circa
Velocità di scansione:	da 48 a 90 fogli A4 al minuto (in funzione della risoluzione e dell'orientamento dei fogli)
Risoluzione max:	300 dpi
Formato output:	immagini TIFF in bianco e nero (fino al 7.10.2013) immagini pdf in bianco e nero (dal 7.10.2103)
Interfaccia:	SCSI II
Accessori installati:	*Patch Reader* per il riconoscimento dei fogli marcatori di inizio/fine documento. *Document printer* per l'apposizione della segnatura di protocollo ai documenti in ingresso.

La soluzione che ha portato l'Ateneo ad adottare la soluzione, previo parere positivo di CNIPA (oggi Agenzia per l'Italia Digitale) richiesto da RSP, presenta i seguenti vantaggi:

- Garanzia di integrità dei documenti registrati: l'acquisizione dell'immagine con segnatura, con l'aggiunta dell'impronta, rende indissolubile l'associazione tra il codice di protocollo ed il documento stesso.
- Efficienza in fase di acquisizione dell'immagine: l'acquisizione dei documenti è veloce in quanto effettuata tramite scanner ad alta produttività, alimentato tramite alimentatore automatico.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Tempestività: contestuale popolamento dell'archivio ottico contenente le immagini dei documenti protocollati per l'immediata disponibilità dell'immagine dei documenti
- Riduzione dei tempi di segnatura: la segnatura viene apposta automaticamente e non comporta dispendio di tempo da parte degli operatori.
- Uniformità di segnatura: apposizione effettuata ad opera di un processo automatico.
- Riduzione degli errori umani in fase di segnatura: si minimizza il rischio di errata apposizione della segnatura.
- Incremento del numero di documenti di cui è acquisita l'immagine nel sistema del PdP.

Le restanti strutture dell'Ateneo (Poli, Facoltà, Dipartimenti, Centri, etc..) dove il numero di pratiche da protocollare non è elevato e non presenta tipicamente i problemi di picco dell'Amministrazione Centrale, la soluzione implementata prevede la seguente sequenza operativa:

1. Registrazione delle informazioni minime di protocollo (metadati);
2. Stampa dell'etichetta con i dati di segnatura;
3. Apposizione dell'etichetta;
4. Acquisizione dell'immagine del documento segnato, calcolo e registrazione dell'hash.

L'acquisizione è in tal caso pilotata direttamente dall'applicazione PdP che offre, inoltre, la possibilità di gestire in differita l'associazione al metadato di protocollo l'immagine del documento collegato, mediante lettura del codice a barre riportata sull'etichetta di protocollo (riportata nell'**allegato 14**). L'operatore di protocollo, abilitato a tale funzionalità, se dotato di uno scanner a fogli multipli, potrà quindi effettuare il completamento delle registrazioni immettendo nel caricatore i documenti protocollati e dotati di segnatura. Il processo di acquisizione del PdP provvede quindi alla acquisizione delle immagini ed alla corretta associazione delle stesse alle rispettive registrazioni di protocollo.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

12. RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

Il presente capitolo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali gestite dal PdP.

12.1. Generalità

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del servizio di protocollo, in base agli UU di appartenenza, ovvero in base alle rispettive competenze (UOP, UOR, UU) hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita, ad esempio, da una componente:
  - ✓ pubblica che permette l'identificazione dell'utente da parte del sistema (userID);
  - ✓ privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RSI, che si avvale di un utente così detto privilegiato (amministratore). Gli utenti del servizio di protocollo, una volta identificati, sono associati ad uno o più specifici profili d'accesso, sulla base delle rispettive competenze.

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli UU e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'Amministrazione sono costantemente aggiornate a cura del RSI, mentre è a cura dell'RSP mantenere costantemente adeguata la configurazione dei profili di abilitazione messi a disposizione degli utenti, con le rispettive specifiche abilitazioni all'utilizzo delle funzioni del PdP.

12.2. Abilitazioni interne ad accedere ai servizi di protocollo

Gli utenti abilitati accedono al PdP mediante username e password, le stesse credenziali personali utilizzate per accedere all'area riservata UNINA e ai servizi

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

istituzionali in essa disponibili.

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

L'Università utilizza un sistema centralizzato per il controllo dell'autenticazione degli utenti, unico per tutte le applicazioni istituzionali, ragion per cui, il PdP non custodisce le password degli utenti. Il controllo di abilitazione è invece eseguito dal PdP, sulla base delle profilature degli utenti. Ciascun utente può essere abilitato ad una o piu' postazioni (le scrivanie) e ne sceglie una nel momento in cui istanzia una sessione di lavoro.

Tutte le utenze dell'Amministrazione sono configurate con un time-out che provvede a disconnettere automaticamente l'applicazione dopo 20 minuti di inattività, così come è riportato nel Piano della sicurezza del sistema in allegato 8.

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

In caso di smarrimento della password, l'utente può provvedere in autonomia, utilizzando il codice puk segreto, al reset password mediante l'apposita funzionalità di "attiva-resetta password" disponibile all'indirizzo https://inbox.unina.it. Nel caso di smarrimento del puk o di attivazione di una nuova identità digitale, all'interessato vengono spedite le credenziali personali in busta chiusa presso la rispettiva struttura di afferenza.

Infine, va segnalato che l'accesso al PdP è consentito solo da postazioni sulla intranet dell'Amministrazione: per collegarsi al sistema del PdP da internet gli utenti devono essere appositamente autorizzati e quindi autenticarsi preventivamente tramite una sessione di tipo "terminal server".

12.3. Profili di accesso

12.3.1 Il conferimento delle abilitazioni

I Responsabili UOR/UU, nominati formalmente Responsabili del trattamento dei dati relativo al proprio ambito, richiedono di autorizzare i propri incaricati ad accedere al PdP, specificandone il livello di autorizzazione all'accesso ai dati (tipicamente quelli della struttura di afferenza) e all'utilizzo di funzioni del PdP. Il modello utilizzato è il SICURDAT/B, pubblicato all'indirizzo:

http://allegati.unina.it/ateneo/modulistica/privacy/

Tale modulo, una volta compilato e sottoscritto dal responsabile UOR/UU viene protocollato e quindi indirizzato dal Responsabile UOR/UU al Direttore Generale per l'autorizzazione. Sempre tramite protocollo, se l'autorizzazione è concessa, il

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

documento viene inviato dalla Segreteria della Direzione Generale al Contact Center del CSI. A questo punto, viene aperto un trouble ticket preso in carica dall'Area tecnica eGovernment del CSI che provvede ad abilitare gli incaricati indicati nel modulo ed autorizzati dal Direttore Generale, utilizzando come nome utente l'identità digitale dell'incaricato. Se l'utente autorizzato non è dotato di identità digitale, il ticket viene preventivamente smistato al gruppo responsabile del processo di creazione dell'identità digitale dell'interessato.

Il processo è analogo per la revoca delle abilitazioni. La cessazione dal servizio determina l'immediata disabilitazione dell'utente ad accedere al PdP.

12.3.2 Utente amministratore di PdP

Ha il compito di condurre il sistema sia dal punto di vista gestionale che dal punto di vista tecnico: configurazione e parametrizzazione dell'applicativo, rilascio password, creazione dei profili delle utenze, attività necessarie all'installazione e alla manutenzione del sistema. Sono amministratori di sistema (AdS) di tipo "SYS", "DBA", "Reti" ed "applicazione" unità di personale del CSI ed il fornitore del servizio di manutenzione del PdP, formalmente nominati con apposito atto da RSI.

In particolare, le abilitazioni degli utenti sono effettuate dagli AdS di tipo "applicazione" del PdP, i componenti dell'Area Tecnica eGovernment. Tali incaricati, utilizzando le proprie credenziali personali, sono in grado di utilizzare specifiche funzionalità del PdP per la creazione, modifica o cessazione di utenti e postazioni di lavoro, sulla base delle richieste contenute nel modello Sicurdat/B, oppure di decreti e comunicazioni che pervengono dall'Amministrazione.

12.3.3 I profili utente

Di seguito, si riportano i codici dei profili di abilitazione ad oggi previsti per l'accesso al sistema di PdP, da riportare nel modulo di autorizzazione SICURDAT/B:

Sigla del profilo	Descrizione della funzionalità
GD	Modifica, annullamento, visualizzazione, presa in carico e movimentazione dei documenti della propria struttura, e di tutte le sotto-strutture. (Solo uffici di Direzione)
GDP	Modifica, annullamento, visualizzazione, presa in carico e movimentazione dei documenti della propria struttura, e di tutte le sotto-strutture. Abilitazione al Protocollo Particolare. (Solo Segreteria Direzione Amm.va)
SG	Modifica, annullamento, visualizzazione, presa in carico e movimentazione dei documenti della propria struttura. Sola visualizzazione dei documenti delle proprie sotto-strutture. (Solo Ripartizioni dell'Amm. Centrale)
PRA	Registrazione di protocollo, modifica, annullamento, visualizzazione, presa in carico e movimentazione dei documenti della propria struttura, e di tutte le sotto-strutture. Completamento dei documenti acquisiti mediante scanner

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Sigla del profilo	Descrizione della funzionalità
	massivo. (Solo Ufficio Protocollo dell'Amm. Centrale)
ASA	Acquisizione e segnatura documenti mediante scanner massivo, assegnazione dei lotti di lavorazione per il completamento della registrazione Gestione dell'annullamento delle registrazioni di protocollo. (Solo Ufficio Protocollo dell'Amm. Centrale)
UF	Visualizzazione, presa in carico e movimentazione dei documenti della propria struttura. (Profilo disponibile per tutti gli uffici e tutte le strutture)
VS	Sola visualizzazione dei documenti dalla propria struttura. (Profilo disponibile per tutti gli uffici e tutte le strutture)
PR	Registrazione di protocollo, modifica, annullamento, visualizzazione, presa in carico e movimentazione dei documenti della propria struttura, e di tutte le sotto-strutture. (Profilo disponibile per tutti gli uffici e per tutte le strutture)
ADM	Tutte le funzionalità della procedura, inclusa la gestione dell'organigramma e dei profili di abilitazione degli utenti e delle postazioni. (Solo CSI)

- **ABILITAZIONI A SPECIFICHE FUNZIONALITÀ (AGGIUNTIVE)**
  (Le abilitazioni a specifiche funzionalità, anche più di una, devono essere indicate in aggiunta al profilo base, nella stessa casella del Sicurdat).

Sigla da riportare nella richiesta	Descrizione della funzionalità
RSV	Abilitazione alla visualizzazione dei documenti riservati della propria struttura
REP	Abilitazione all'utilizzo di repertori. In tal caso, indicare - tra parentesi - anche la sigla dei repertori di competenza. L'elenco completo ed aggiornato dei repertori disponibili è consultabile all'indirizzo: http://www.praxis.unina.it/protocollo-sistema-ateneo
SCAN	Funzionalità si scansione massiva presso dipartimenti (Scanprot)
DK	Accesso al sistema di protocollo tramite connessione internet remota
CC	Copia Conforme automatizzata

12.4. Modalità di creazione e gestione delle utenze e dei relativi profili di accesso

Per la creazione e l'amministrazione delle utenze e password l'AdS-Applicazione del protocollo utilizza funzionalità di amministrazione presenti nel PdP.

Il profilo associato ad un utente consente di definire i permessi che questi ha relativamente ai seguenti aspetti:

a) Gestione dei documenti e dei fascicoli. La gestione comprende le seguenti operazioni:
   - Completare i dati di un documento, cioè classificare e fascicolare qualora questo non sia già stato fatto

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Modificare i dati non "annullabili", compresa la classificazione e fascicolazione
- Smistare o inviare i documenti/fascicoli ad altri uffici/scrivanie
- Creare copie
- Modificare i permessi al documento/fascicolo
- Riaprire o chiudere il fascicolo

b) Abilitazioni alle funzionalità del sistema

c) Abilitazioni a certe tipologie di dati particolari

Con particolare riguardo al punto a), le 2 possibilità principali del sistema sono:

1. Abilitare un utente a gestire solo i documenti/fascicoli assegnati alla propria scrivania
2. Abilitare un utente a gestire sia i documenti/fascicoli assegnati alla propria scrivania sia i documenti/fascicoli assegnati al proprio ufficio di appartenenza.

La gestione della sicurezza comprende comunque anche una sezioni di abilitazione alle varie funzionalità del sistema: protocollazione, iter documentale, repertoriazione, funzionalità speciali, etc. In particolare, ogni utente potrebbe essere abilitato solo a certe funzionalità del sistema e non ad altre (per esempio alle funzionalità speciali, come l'annullamento delle registrazioni, l'annullamento dei dati "annullabili", etc, normalmente non vengono abilitati tutti gli utenti del sistema ma solo un piccolo sottoinsieme).

Infine, un altro aspetto di sicurezza (punto c)) è connesso alle abilitazioni a certe tipologie di dati particolari quali, ad esempio:

- I repertori: possono essere cioè definiti repertori a cui sono abilitati alla registrazione/visualizzazione solo a determinati uffici/postazioni, oppure esclusi altri in modo esplicito;
- Le voci di titolazione: possono essere assegnate e abilitate all'utilizzo anche solo a determinate scrivanie/uffici. Inoltre si può abilitare solo determinate scrivanie/uffici alla fascicolazione su voci di titolario.

12.5. Abilitazioni esterne (privati)

Alla data, l'Amministrazione non concede autorizzazioni di accesso al PdP a soggetti (privati) esterni all'Amministrazione. È infatti l'URP (Ufficio Relazioni con il Pubblico) dell'Amministrazione Centrale l'ufficio incaricato di gestire la comunicazione con i soggetti abilitati alla consultazione dei dati propri presenti all'interno dell'Amministrazione e di fornire loro tutte le informazioni ed i documenti amministrativi a cui hanno il diritto di accedere.

12.6. Abilitazioni esterne concesse ad altre AOO

Alla data, l'Amministrazione non concede autorizzazioni di accesso al PdP ad altre

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

amministrazioni.

12.7. Consultazione delle registrazioni di protocollo particolari

Il complesso dei documenti per i quali è stata attivata la registrazione di protocollo particolare costituisce l'archivio particolare.
I documenti e i fascicoli dell'archivio particolare sono consultabili nel rispetto delle seguenti norme:

- art. 24 della legge 07 agosto 1990, n. 241, e successive modificazioni;
- art. 8 del decreto del Presidente della Repubblica 27 giugno 1992, n. 352;
- artt. 107 e 108 del decreto legislativo 29 ottobre 1999, n. 490.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

13. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

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

13.1. Il registro di emergenza

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

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

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

Il registro di emergenza si configura come un repertorio del protocollo generale, identificato da codici il cui prefisso è "RE", uno per ciascuna UOR. L'elenco dei codici di registro di emergenza associati a ciascuna UOR (uno per ciascuna postazione di protocollo configurata) è riportato nell'**allegato 3**. RSP garantisce l'unicità dell'associazione di tale codice.

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza. I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

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

Il RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica centralizzata, le operazioni di apertura del registro di emergenza e di protocollo sono svolte su postazioni di lavoro operanti fuori linea, attraverso l'uso del software "E-Grammata Protocollo di emergenza" predisposta da RSP. Tale applicazione viene eseguita su postazioni preventivamente istallate e configurate (almeno una per ciascuna UOP dotata di proprio Ufficio/Servizio di Protocollo) e consente l'automatico e sicuro caricamento delle registrazioni di emergenza nel PdP

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

non appena sono ristabilite le condizioni per il corretto funzionamento del sistema.

L'utilizzo di questo software, già installato sulla postazione dell'incaricato addetto alla protocollazione, consente di lavorare su un computer anche non collegato alla rete per effettuare le operazioni di protocollo.

Il software esegue le registrazioni utilizzando il codice del registro di emergenza associato alla singola postazione nell'ambito della data UOR.

E' bene precisare che il ricorso a tale procedura si giustifica nella circostanza in cui

a. il sistema di protocollo generale risulta non disponibile per problemi di rete ;
b. il sistema di protocollo generale risulta non disponibile per problemi di sistema.

Nei casi indicati al punto a) e b) l'eventuale indisponibilità o malfunzionamento della postazione di protocollazione di una UOR/UO (che non consentono di utilizzare il software di emergenza), richiedono l'intervento del servizio di assistenza CSI che si raccomanda pertanto di contattare ai fini della risoluzione del problema.

13.2. Modalità di apertura del registro di emergenza

Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, i responsabili UOR/UOP devono richiedere parere a RSP, in merito ai motivi che determinano l'interruzione di servizio, alle previsioni di ripristino della completa funzionalità del sistema on line e quindi, in merito all'opportunità di avviare la procedura di protocollazione in emergenza.

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

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

Il Responsabile della struttura autorizza (con atto da lui sottoscritto) lo svolgimento delle operazioni di protocollo sul registro di emergenza (a norma dell'articolo 63 del DPR 455/2000) nel quale dovranno essere annotate la data, l'ora e la causa dell'interruzione del servizio di protocollo generale.

A tal fine il protocollista, a valle dell'autorizzazione ricevuta, dovrà protocollare l'atto stesso (seguendo la procedura di seguito descritta), prima di procedere con nuove registrazioni di protocollo.

Nella fase di registrazione dell'atto, l'operatore di protocollo dovrà inserire le seguenti

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

informazioni:

1) Nel campo mittente e destinatario, la propria UOR
2) Nel campo oggetto, l'oggetto dell'atto di autorizzazione la data e l'ora di apertura del registro di emergenza, nonché la causa dell'interruzione del servizio di protocollo generale.

13.3. Modalità di utilizzo del registro di emergenza

L'utilizzo di un registro di emergenza separato per ciascuna UOR e la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'Amministrazione.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo generale. Prima di avviare il software di emergenza è buona norma verificare che la data e l'ora della postazione di protocollazione siano impostate correttamente. Le indicazioni operative su come effettuare una registrazione in emergenza sono riportate nell'apposita guida consultabile sul sito Praxis, nella sezione Protocollo Informatico/Manuali e Guide.

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

13.4. Modalità di chiusura e recupero del registro di emergenza

Al ripristino della funzionalità del sistema di protocollo generale, è necessario attuare le seguenti operazioni:

1. Chiudere il registro di emergenza se ancora aperto;
2. Inviare al sistema di protocollo generale le informazioni relative ai documenti protocollati in emergenza (operazione da eseguire obbligatoriamente prima di procedere, con nuove registrazioni di protocollo) utilizzando la funzione di recupero dei dati;
3. Completare le registrazioni di protocollo.

Il registro di emergenza si configura come un repertorio del protocollo generale di Ateneo: ad ogni registrazione recuperata dal registro di emergenza è attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

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

L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza e a quel numero deve farsi riferimento per l'avvio dei termini del procedimento amministrativo.

Una volta ripristinata la piena funzionalità del sistema di Protocollo Generale, il Responsabile della UOR/UO provvede quindi (con apposito atto da lui sottoscritto), alla chiusura del registro di emergenza, annotando sullo stesso il numero delle registrazioni effettuate, la data e l'ora di chiusura del registro.

Il protocollista, a valle del processo di autorizzazione, dovrà effettuerà la registrazione di protocollo dell'atto stesso, immettendo in fase di registrazione le seguenti informazioni:

1. nel campo mittente e destinatario, il codice identificativo della propria UOR/UO;
2. nel campo oggetto, l'oggetto della nota di autorizzazione, nonché il numero delle registrazioni effettuate in emergenza e la data e l'ora di chiusura del registro di emergenza.

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

Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza (postazione di lavoro stand alone) a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza su una o più postazione di lavoro sono inserite nel sistema informatico di protocollo generale utilizzando un'apposita funzione di recupero dei dati.

13.5. Modalità di completamento delle registrazioni di emergenza

Infine, per completare le registrazioni di protocollo effettuate in emergenza sarà necessario:

1 Acquisire l'immagine dei documenti protocollati, inserendole nell'archivio centralizzato per il successivo reperimento e per la consultazione da parte degli utenti abilitati;

2 Se necessario, modificare la UOR/UO di destinazione nel caso delle registrazioni interne-tra uffici se la registrazione in emergenza non conteneva l'insieme di tutte le strutture destinatarie.

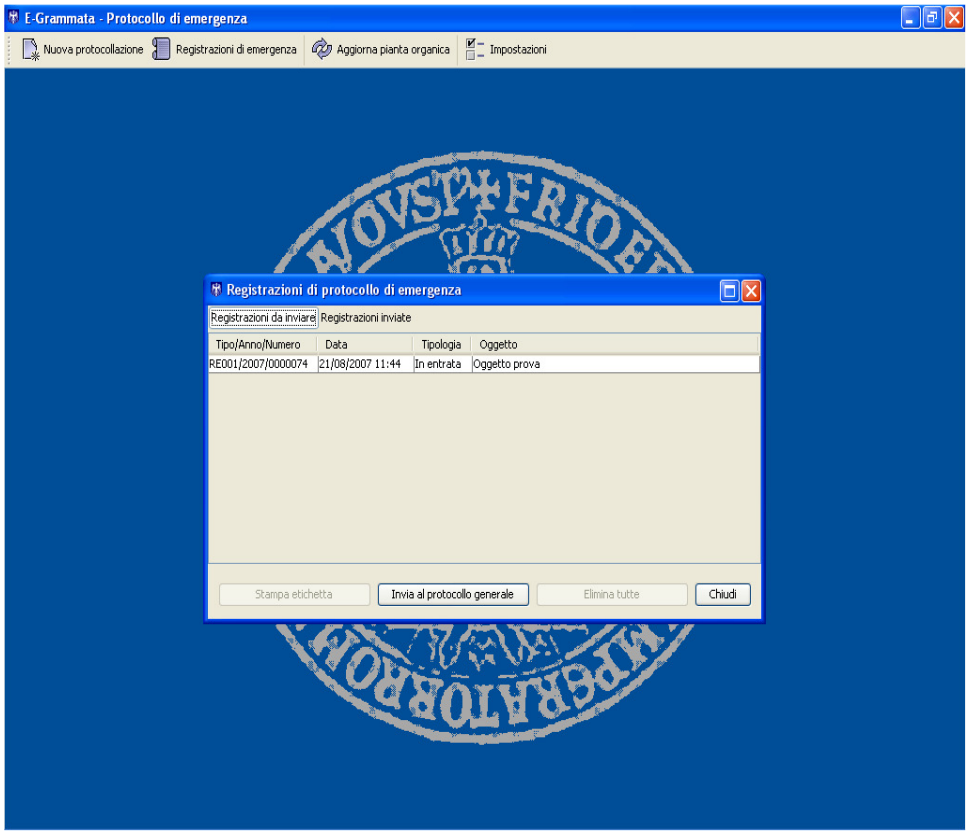
UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

13.6. Il registro dei protocolli di emergenza

Il client di emergenza offre due funzionalità:

- la visualizzazione dell'elenco delle registrazioni ancora da inviare al PdP
- la visualizzazione dell'elenco delle registrazioni già inviate e quindi dotate anche di codice PG.

In entrambi in casi, sono mostrate le seguenti informazioni: Codice di protocollo di emergenza, data ed oggetto della registrazione. Per quelle inviate, anche il codice PG associato.



Inoltre, il registro di protocollo prodotto a partire dal PdP contiene, per ciascuna registrazione l'evidenza del codice di registrazione di emergenza.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

14. GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI

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

14.1. Matrice delle correlazioni

I procedimenti amministrativi sono descritti nel "Catalogo dei procedimenti amministrativi", di cui l'Amministrazione cura l'aggiornamento, estemporaneo o periodico. I procedimenti amministrativi costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'Amministrazione. All'interno del catalogo i procedimenti sono individuati mediante la definizione dei riferimenti riportati al successivo paragrafo 14.2. La definizione del singolo procedimento amministrativo rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa. Il risultato concreto di questa attività sono i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare. L'individuazione del RPA e del responsabile dell'adozione del provvedimento finale è effettuata sulla base delle competenze assegnate a ciascuna figura interna agli UOR/UU.

14.2. Catalogo dei procedimenti amministrativi

La gestione delle attività e dei procedimenti amministrativi, il loro iter, l'individuazione del responsabile del provvedimento finale e i termini entro i quali il procedimento deve essere concluso sono definiti così come previsto da norme di rango legislativo, regolamentare nonché dal regolamento interno emanato dall'amministrazione. A tal fine l'AOO, per favorire la trasparenza dell'azione amministrativa, per semplificare i procedimenti e per schematizzare le descrizioni, costituisce una base informativa dei procedimenti amministrativi registrando, per ciascuno di essi, almeno, le seguenti informazioni:

- la denominazione del procedimento;
- il codice del procedimento;
- i fondamenti giuridici del procedimento;
- le fasi operative del procedimento (e, all'occorrenza, dei sub-procedimenti) e la relativa sequenza;
- UOR/UU competenze per ciascuna fase; il tempo massimo di definizione dell'intero procedimento;
- il tempo di svolgimento di ciascuna fase;
- la forma e il contenuto dei documenti intermedi e del provvedimento finale;
- il responsabile dell'adozione del provvedimento finale;
- il responsabile del procedimento amministrativo;
- il funzionario incaricato dell'istruttoria;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- il titolario a cui il procedimento si riferisce, se disponibile.

L'elenco dei procedimenti amministrativi è contenuto nell'Allegato 1 al Regolamento di Ateneo in materia di procedimento amministrativo e di diritto di accesso ai documenti ed è stato emanato con DR 3142 del 30.09.2013.

14.3. Avvio dei procedimenti e gestione degli stati di avanzamento

Mediante l'assegnazione dei fascicoli agli UOR/UU di volta in volta competenti, le UOP o i RPA provvedono a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente. La registrazione degli stati di avanzamento dei procedimenti amministrativi sulla base informativa sopra richiamata può avvenire in modalità manuale o automatica. Nel primo caso, gli stati di avanzamento sono aggiornati dal RPA. Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

15. AGGIORNAMENTO DEL MANUALE

15.1. Modalità di aggiornamento e approvazione del Manuale

L'Amministrazione adotta con decreto del Direttore Generale il presente "Manuale di gestione del Protocollo Informatico, dei documenti, dell'archivio dell'Università degli Studi di Napoli Federico II", redatto dal Responsabile del Servizio di Coordinamento del Protocollo Informatico (RSP) e integrato con i contributi di revisione forniti dagli uffici e dalle strutture dell'Ateneo che, vista la tematica trattata, sono maggiormente coinvolti nella gestione operativa e informatica dei documenti e degli archivi (analogici e informatici): la Ripartizione Affari legali, Procedure elettorali e Attività di valutazione con l'Ufficio Protocollo e l'Ufficio Archivio, nonché il Centro di Ateneo per i Servizi Informativi (CSI) e il Centro di Ateneo per le Biblioteche (CAB).

Il presente manuale potrà essere aggiornato a seguito di:

- modifiche normative o regolamentari sopravvenute;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- sostanziali modifiche apportate nell'ambito dell'architettura di servizio.

Non ha invece impatto sulla riedizione del presente Manuale l'aggiornamento delle informazioni di carattere "dinamico" (quali, ad esempio, il Titolario, l'Organigramma, l'elenco dei Registri di Protocollo di emergenza, etc.), la cui versione più aggiornata è pubblicata sul sito www.praxis.unina.it. Analogamente, non determinano l'aggiornamento del presente manuale gli adeguamenti tecnologici e informatici che non modificano le politiche generali di gestione e di sicurezza del sistema

La tenuta del presente manuale è affidata al RSP che sottoporrà le nuove versioni del Manuale all'approvazione ed autorizzazione da parte del Direttore Generale.

15.2. Pubblicità del presente Manuale

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1900, n. 241, è reso disponibile alla consultazione del pubblico e di tutto il personale dell'Amministrazione che ne può prendere visione in qualsiasi momento. A tal fine, viene pubblicato sul sito dell'eGovernment di Ateneo raggiungibile dalla *home page* del portale dell'Amministrazione, al seguente indirizzo:

http://www.praxis.unina.it/egov-atti-e-norme.

Inoltre copia del presente Manuale è inviata, per opportuna conoscenza, all'Agenzia per l'Italia digitale, Centro di competenza sul protocollo informatico.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Allegati

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

INDICE DEGLI ALLEGATI

A1. DEFINIZIONI 134

A2. NORMATIVA DI RIFERIMENTO 146

A2.1. LEGGI E NORME 146
A2.2. REGOLAMENTI E ATTI DELL'ATENEO 148

A3. AREA ORGANIZZATIVA OMOGENEA E CARATTERISTICHE ORGANIZZATIVE 151

A3.1. DATI IDENTIFICATIVI DELL'AMMINISTRAZIONE 151
A3.2. CARATTERIZZAZIONE DELL'AREA ORGANIZZATIVA OMOGENEA 151
A3.3. ORGANIGRAMMA DEL PROTOCOLLO INFORMATICO 152
A3.4. UOR E RELATIVI CODICI DI REGISTRO EMERGENZA 158

A4. ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO DI COORDINAMENTO DEL PROTOCOLLO INFORMATICO 162

A5. I TITOLARI DI FIRMA DIGITALE 166

A6. PIANO FORMATIVO PER IL PERSONALE DELL'AMMINISTRAZIONE PER L'AVVIO DEL SISTEMA 167

A6.1. I MODULI FORMATIVI 167
A6.2. I PROFILI DEI FRUITORI DEI CORSI 168
A6.3. I PERCORSI FORMATIVI 169
A6.4. DETTAGLIO DEL CONTENUTO DEI CORSI 170

A7. PIANO DI ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO 173

A8. MISURE DI SICUREZZA 180

A8.1. L'ARCHITETTURA TECNICA DEL SISTEMA 180
A8.2. L'ARCHITETTURA APPLICATIVA 181
A8.3. L'ARCHITETTURA DI SICUREZZA 182
A8.3.1 Le funzioni di sicurezza 182
A8.3.2 Descrizione generale dei meccanismi di sicurezza implementati nel PdP 184
A8.3.3 Le funzioni di sicurezza di tipo informatico 186
A8.3.4 Componente organizzativa della sicurezza 196
A8.3.5 Componente infrastrutturale della sicurezza 199
A8.3.6 Le minacce e gli agenti 201
A8.3.7 La tabella di correlazione minacce/funzioni di sicurezza 202
A8.3.8 Determinazione del grado di copertura e del rischio residuo 204

A9. CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO 206

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A10.ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO 209
A10.1. DOCUMENTI IN ARRIVO 209
A10.2. DOCUMENTI IN PARTENZA 210
A10.3. DOCUMENTI INTERNI 210
A10.4. ECCEZIONI 210
A11.ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE 211
A12.TITOLARIO DI CLASSIFICAZIONE 212
A13.REPERTORI GENERALI 216
A14.ELEMENTI DELLA SEGNATURA DI PROTOCOLLO PER LA CORRISPONDENZA CARTACEA 217
A14.1 ESEMPIO DI SEGNATURA PRODOTTA DAGLI SCANNER MASSIVI 217
A14.2 ESEMPIO DI SEGNATURA PRODOTTA DAGLI SCANNER PRESSO LE UOR DIVERSE DALL'AMMINISTRAZIONE CENTRALE 217
A14.3 IL TIMBRO DIGITALE 218

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A1. DEFINIZIONI

Oggetto/Soggetto	Descrizione
AMMINISTRAZIONI CERTIFICANTI	Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti (art. 1, comma 1,lett. p) del DPR n. 445/2000);
AMMINISTRAZIONI PROCEDENTI	Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio (art. 1, comma 1 lett. o) DPR n.445/2000);
AMMINISTRAZIONI PUBBLICHE	Per amministrazioni pubbliche si intendono quelle indicate nell'art. 1, comma 2 del d.. lgs.30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI	le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (art. 1, comma1 lett. z) del d. lgs.7 marzo 2005, n.82)
ARCHIVIO	L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dell'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione o dalla Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico-culturale. L'archivio è unico. Per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio il legislatore ha previsto la sua suddivisibilità in tre sezioni: archivio corrente, archivio generale o di deposito e sezione separata dell'archivio generale o archivio storico;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
ARCHIVIO CORRENTE	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;
ARCHIVIO GENERALE O DI DEPOSITO	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;
SEZIONE SEPARATA DELL'ARCHIVIO GENERALE O ARCHIVIO STORICO	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne;
ARCHIVIAZIONE ELETTRONICA	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (art.1 della Deliberazione CNIPA 19 febbraio 2004 n.11);
AREA ORGANIZZATIVA OMOGENEA (AOO)	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato (art.2, lett. n) del DPCM 31 ottobre 2000);
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive .(art 1., comma 1, lett.i) del DPR 28 dicembre 2000, n. 445);
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; (art. 1, comma 1 lett.b) del d. lgs.7 marzo 2005, n.82);

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art.4 comma 1 lett.o) del d. lgs 30 giugno 2003 n.196);
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (art.4, comma 1, lett. d) del d. lgs 30 giugno 2003 n. 196);
CARTA NAZIONALE DEI SERVIZI	il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (art. 1 del d. lgs.7 marzo 2005, n. 82);
CARTA D'IDENTITÀ' ELETTRONICA	il documento d'identità' munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità' anagrafica del suo titolare(art. 1comma 1, lett. c) del d.lgs. 7 marzo 2005, n. 82) ;
CASELLA DI POSTA ELETTRONICA ISTITUZIONALE	la casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del D.P.C.M. 31 ottobre 2000, articolo 15, comma 3).(art.1 dell'allegato A alla circolare AIPA 7 maggio 2001 n. 28);
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (art. 1, comma 1 lett. e) del Dlgs. 7 marzo 2005, n. 82)
CERTIFICATO QUALIFICATO	il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art. 1 comma 1 lett.f) del Dlgs.7 marzo 2005, n. 82)
CERTIFICATO	Il documento rilasciato da una Amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (art.1comma 1 lett.f) del DPR 28 dicembre 2000, n. 445);

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
CERTIFICATORE	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime(art. 1, comma 1 lett.g) del Dlgs. 7 marzo 2005, n. 82);
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 comma 1 lett. l) del d. lgs. 30 giugno 2003 n. 196);
CONSERVAZIONE SOSTITUTIVA	Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004; n.11;
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art.4 comma 3 lett.d) del d. lgs. 30 giugno 2003 n.196);
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art.4, comma 1 lett. e) del d.lgs. 30 giugno 2003 n. 196);
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato (art.4, comma 1 lett.c) del d. lgs. 30 giugno 2003 n. 196);
DATI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art.4 comma 1, lett. ddd) del d. lgs. 30 giugno 2003 n. 196);

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art.4 comma 1 lett.n) del d.lgs. 30 giugno 2003 n. 196);
DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art.4 comma 1 lett.b) del d.lgs. 30 giugno 2003 n. 196);
DATO PUBBLICO	il dato conoscibile da chiunque (art. 1comma 1 lett.n) del d. lgs. 7 marzo 2005, n. 82);
DATO A CONOSCIBLITÀ LIMITATA	il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. 1comma 1 lett.l) del d. lgs. 7 marzo 2005, n. 82;)
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal art.1 comma 1 lett.h) del DPR 28 dicembre 2000, n. 445;
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato .(art.1 comma 1 lett. g) del DPR 28 dicembre 2000, n. 445);
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art.4 del d.lgs. 30 giugno 2003 n. 196);
DOCUMENTO	Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (art 1.comma 1 lett.a) Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.(art.1 comma 1 lett.a) del DPR 28 dicembre 2000, n. 445);

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
DOCUMENTO ANALOGICO	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art 1comma 1 lett.b). Deliberazione CNIPA del 19 febbraio 2004, n. 11);
DOCUMENTO ANALOGICO ORIGINALE	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art 1. Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (art 1.comma 1 lett.h) Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO CONSERVATO	Documento sottoposto al processo di conservazione sostitutiva (art 1. Deliberazione CNIPA del 19 febbraio 2004 n. 11);
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare .(art.1comma 1 lett.c) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica Amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare .(art.1comma 1 lett.d) del DPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITÀ ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (art.1comma 1 lett..e) del DPR 28 dicembre 2000, n.445);
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. t) del Dlgs.7

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	marzo 2005, n. 82);
DOSSIER	È una aggregazione di più fascicoli che può essere costituito a seguito di esigenze operative dell'Amministrazione, come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona;
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia (art.1comma 1 lett. n) della deliberazione AIPA 19 febbraio 2004 n. 11);
EVIDENZA INFORMATICA	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art.1 comma 1 , lett.f) del DPCM 13 gennaio 2004) ;
FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi
FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento;
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lett.s) del Dlgs.7 marzo 2005, n. 82);
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lett.q) del Dlgs.7 marzo 2005, n. 82);
FIRMA ELETTRONICA QUALIFICATA	la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1 comma 1 lett.r) del Dlgs.7 marzo 2005, n. 82);
FORMAZIONE DEI DOCUMENTI INFORMATICI	Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa.(art.2 della deliberazione AIPA 23 novembre 2000 n. 51);
FUNZIONE DI HASH	una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (art.1 comma 1 lett.e) del DPCM 13 gennaio 2004);
GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del Dlgs 30 giugno 2003 n.196, istituita dalla legge 31 dicembre 1996, n. 675 (art.4 comma 1 lett.q) del d.lgs. 30 giugno 2003 n. 196);
GESTIONE INFORMATICA DEI DOCUMENTI	l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1 comma lettl del d. lgs. 7 marzo 2005, n. 82);
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art.1 del DPCM 13 genaio 2004);
INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
INSERTO	È un sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (art.1 comma 1 lett . l) del DPR 28 dicembre 2000, n. 445);
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica Amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato.(art.1 comma 1 lett.n) del DPR 28 dicembre 2000, n. 445);
MARCA TEMPORALE	un'evidenza informatica che consente la validazione temporale (art.1comma 1 lett.i) del DPCM 31 gennaio 2004);
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sottopartizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascun procedimento/procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello stato o per la sezione degli archivi storici per gli Enti Pubblici) e quali invece possono

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il PIANO DI CONSERVAZIONE periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
MEMORIZZAZIONE	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del decreto legislativo 23 gennaio 2002, n. 10 (art 1, comma 1, lett.f) Deliberazione CNIPA del 19 febbraio 2004 n.11);
MISURE MINIME DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del d.lgs 30 giugno 2003 n. 196. (art.4 comma 3 lett. a) del d.lgs. 30 giugno 2003 n. 196);
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica (art.4, comma 3, lett. e) del d. lgs 30 giugno 2003, n. 196);
ORIGINALI NON UNICI	i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art 1. , comma 1, lett. v) del d. lgs.7 marzo 2005, n. 82);
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	Vedi MASSIMARO DI SELEZIONE E SCARTO
PROFILO DI AUTORIZZAZIONE	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (art.4, comma 3, lett. f) del d. lgs. 30 giugno 2003 n. 196);
PUBBLICO UFFICIALE	Il notaio, salvo quanto previsto dall'art. 5, comma 4 della Deliberazione CNIPA del 19 febbraio 2004, n. 11 e nei casi per i quali possono essere chiamate in causa le altre figure

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (art 1. Deliberazione CNIPA del 19 febbraio 2004, n. 11);
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art.4, comma 1, lett. g) del d. lgs. 30 giugno 2003 n. 196);
RESPONSABILE DEL SERVIZIO DI PROTOCOLLO	Il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'articolo 62, comma 2, del DPR 28 dicembre 2000, n. 445;
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI (RPA)	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente
RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art 1,, comma 1, lett. g) del DPCM 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (art.1, comma 1, lett. i), del DPR 11 febbraio 2005, n.68)
RIVERSAMENTO DIRETTO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (art , comma 1, lett. n) . Deliberazione CNIPA del 19 febbraio 2004, n. 11)
RIVERSAMENTO SOSTITUTIVO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (art 1., comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11)
SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (art.4, comma 4, lett. c) del d. lgs. 30 giugno 2003 n. 196)
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (art.4,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Oggetto/Soggetto	Descrizione
	comma 4, lett. b) del d.lgs. 30 giugno 2003 n. 196);
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (art.4, comma 4, lett. a) del Dlgs 30 giugno 2003 n. 196);
SEGNATURA INFORMATICA	l'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'articolo 18, comma 1, del D.P.C.M. 31 ottobre 2000 (art.1 dell'allegato A della circolare AIPA 7 maggio 2001 n. 28);
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (Glossario dell'IPA Indice delle Pubbliche Amministrazioni);
SISTEMA DI CLASSIFICAZIONE	lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (art.2, comma 1, lett. h) del DPCM 31 ottobre 2000);
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art.4, comma 3, lett. g) del d.lgs. 30 giugno 2003 n. 196);
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1., comma 1, lett. r) del DPR 28 dicembre 2000 n. 445);
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A2. NORMATIVA DI RIFERIMENTO

A2.1. Leggi e norme

1. Legge 7 agosto 1990, n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192)
2. D.P.R. 27 giugno 1992, n. 352 - Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. 29 luglio 1992, n. 177)
3. D.P.R. 12 febbraio 1993, n. 39 - Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera m), della legge 23 ottobre 1992, n. 421. (G.U. 10 febbraio 1993, n. 42)
4. D.P.C.M. 28 ottobre 1999 - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
5. Decreto legislativo 29 ottobre 1999, n. 490 - Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352. (GU. 27 dicembre 1999, n. 302)
6. D.P.C.M. 31 ottobre 2000 - Regole tecniche per il protocollo informatico; valido ai sensi dell'art. 78 del D.P.R. 20 ottobre 1998, n. 428. (G.U. n. 272 del 21 novembre 2000)
7. Deliberazione AIPA 23 novembre 2000, n. 51- Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del D.P.R. 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291)
8. D.P.R. 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
9. Circolare del 16 febbraio 2001, n. AIPA/CR/27 – "Art. 17 del DPR 10 novembre 1997, n. 513 - Utilizzo della firma digitale nelle pubbliche amministrazioni".
10. Circolare del 21 giugno 2001, n. AIPA/CR/31 – "Art. 7, comma 6, del decreto del Presidente del Consiglio dei ministri del 31 ottobre 2000, recante "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente".
11. Decreto legislativo 30 marzo 2001, n. 165 - "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".
12. Circolare AIPA 7 maggio 2001, n. AIPA/CR/28 - Articolo 18, comma 2, del DPCM 31 ottobre 2000 Recante regole tecniche per il protocollo informatico di cui al D.P.R. 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. (G.U. 21 novembre 2000, n. 272)

13. Circolare AIPA 21 giugno 2001, n. AIPA/CR/31 (Art. 7, comma 6, del D.P.C.M. 31 ottobre 2000 recante "Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili.)
14. Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001 - Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
15. Direttiva 16 gennaio 2002, Dipartimento per l'innovazione e le tecnologie - Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.
16. Decreto legislativo 23 gennaio 2002, n. 10 - Recepimento della direttiva 1999/93/CE sulla firma elettronica.
17. Direttiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002 - Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
18. Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002 - Linee guida in materia di digitalizzazione dell'amministrazione.
19. Legge 27 dicembre 2002, n. 289 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
20. D.P.R. 7 aprile 2003, n. 137 - Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002.
21. Decreto legislativo 30 giugno 2003, N. 196 - Codice in materia di protezione dei dati personali.
22. Decreto Ministeriale 14 ottobre 2003 - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23. Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003 - Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
24. Direttiva 18 dicembre 2003 - Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
25. D.P.C.M. 13 gennaio 2004 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98)
26. Deliberazione CNIPA 19 febbraio 2004, n. 11 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali
27. Decreto legislativo 22 gennaio 2004, n. 42 - Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28)
28. Decreto del presidente del Consiglio dei Ministri 13 gennaio 2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

riproduzione e la validazione, anche temporale, dei documenti informatici (G.U. 27 aprile 2004, n. 98)

29. Decreto legislativo 28 febbraio 2005, n. 42 – Istituzione del sistema pubblico di connettività e della rete internazionale della PA, ai sensi dell'art. 10 della legge 29 luglio 2003, n. 229 (G.U. 30 marzo 2005, n. 73)
30. Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (G.U. 16 maggio 2005, n. 112)
31. Legge n. 2 del 28 gennaio 2009 - Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (G.U. 28 gennaio 2009 n. 22 - supp. ordinario n. 14)
32. Decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici (G.U. n. 219 del 6 giugno 2009)
33. Deliberazione CNIPA n. 45 del 21 maggio 2009, modificata dalla Determinazione DigitPA n. 69 del 28 luglio 2010 - Regole per il riconoscimento e la verifica del documento informatico
34. Legge n. 69 del 18 giugno 2009 - Disposizione per lo sviluppo economico, la semplificazione, la competitività nonchè in materia di processo civile (G.U. 19 giugno 2009, n. 140 - supp. ordinario n. 95)
35. Legge n. 69 del 18 giugno 2009 - Disposizione per lo sviluppo economico, la semplificazione, la competitività nonchè in materia di processo civile (G.U. 04 agosto 2009, n. 179 - supp. ordinario n. 140)
36. Legge n. 102 del 03 agosto 2009 - Conversione in legge, con modificazioni, del decreto-legge 1° luglio 2009, n. 78, recante provvedimenti anticrisi, nonché proroga di termini e della partecipazione italiana a missioni internazionali (G.U. 04 agosto 2009, n. 179 - supp. ordinario n. 140)
37. Decreto legislativo n. 150 del 27 ottobre 2009 - Attuazione legge 4 marzo 2009 n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle PA (G.U. 31 ottobre 2009, n. 254)
38. Decreto legislativo n. 179 del 18 ottobre 2012 - Ulteriori misure urgenti per la crescita del Paese (G.U. n. 179 del 18 dicembre 2012)
39. Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (G.U. n. 117 del 21 maggio 2013)
40. Circolare n. 62/2013 dell'Agenzia per l'Italia Digitale recante le "Linee guida per il contrassegno generato elettronicamente".

A2.2. Regolamenti e Atti dell'Ateneo

1. Regolamento di Ateneo UNINA titolato "Regolamento di attuazione del Codice di protezione dei dati personali utilizzati dall'Università degli Studi di Napoli Federico II", emanato con D.R. n. 5073 del 30.12.2005.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

2. Regolamento di Ateneo UNINA titolato "Regolamento in materia di Firma Digitale", emanato con D.R. n. 4064 del 31.10.2006.

3. Regolamento di Ateneo UNINA titolato "Regolamento per l'utilizzo del servizio di Posta elettronica @unina.it", emanato con D.R. n. 4489 del 29.12.2010.

4. Regolamento di Ateneo UNINA titolato "Regolamento in materia di Posta Elettronica Certificata", emanato con D.R. n. 1614 del 11.05.2012.

5. Ordine di Servizio n. 246 del 19.12.2012 relativo alla "Gestione digitale dell'iter di emanazione e di registrazione dei decreti dirigenziali".

6. Ordine di Servizio n. 200 del 23.11.2012 contenente "Nuove indicazioni operative per l'utilizzazione della funzionalità "apponi timbro" disponibile nel Sistema di Protocollo Informatico".

7. Ordine di Servizio n. 345 del 6.12.2011 riguardante "L'avvio all'iter informatico di emanazione e registrazione degli Ordini di Servizio del Direttore Amministrativo".

8. Ordine di Servizio n. 51 del 3.04.2012 contenente "Modifiche al flusso operativo della registrazione di protocollo e trasmissione degli atti legali notificati".

9. Ordine di Servizio n. 92 del 7.04.2011 contenente "Chiarimenti sulla copertura finanziaria mediante riaccertamento in conto residui della Contabilità Speciale Gestione Stralcio ex Policlinico Universitario".

10. Ordine di Servizio n.72 del 10.03.2011 contenente "Chiarimenti in ordine al flusso relativo ai decreti del Rettore e del Direttore Amministrativo con impegno di spesa".

11. Ordine di Servizio n. 25 del 21.01.2011 contenente "Disposizioni per la produzione di copie conformi dei decreti digitali".

12. Ordine di Servizio n. 44 del 04.02.2011 contenente "Ulteriori disposizioni connesse all'avvio del nuovo iter per l'emanazione dei decreti digitali".

13. Ordine di Servizio n. 400 del 23.12.2010 (e s.m.i.: OdS n. 408 del 28.12.2010 e OdS n. 29 del 25.01.2011) recante le "Disposizioni in materia di digitalizzazione dei decreti rettoriali e direttoriali".

14. Ordine di Servizio n. 149 del 04.06.2010 contenente "Nuove modalità di trasmissione dei provvedimenti di competenza dell'Ufficio Statuto, Regolamenti ed Organi Universitari".

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

15. Ordine di Servizio n. 352 del 02.12.2009 contenente "Protezione dati personali. Revoca delle disposizioni dettate dall'OdS n. 372 del 13.10.2008 (Disposizioni in materia di gestione dei flussi documentali) in ordine alla trasmissione dei modelli Sicurdat A e B. Nuove disposizioni".

16. Ordine di Servizio n. 221 del 28.07.2009 contenente "Attivazione repertorio e protocollazione degli atti legali notificati".

17. Ordine di Servizio n. 220 del 28.07.2009 contenente "Attivazione indirizzo PEC di Ateneo".

18. Ordine di Servizio n. 219 del 28.07.2009 contenente "Flusso operativo per la protocollazione di messaggi PEC".

19. Ordine di Servizio n. 372 del 13.10.2008 contenente "Disposizioni in materia di flussi documentali".

20. Ordine di Servizio n. 159 del 03.06.2008 contenente "Emanazione del nuovo Titolario dell'Università degli Studi di Napoli Federico II".

21. Ordine di Servizio n. 198 del 17.07.2007 contenente "Chiarimenti sulla gestione del flusso operativo dei documenti protocollati inviati da altre strutture dell'Ateneo agli uffici dell'Amministrazione Centrale".

22. Ordine di Servizio n. 160 del 12.06.2007 contenente "Diffusione del sistema di Protocollo Informatico di Ateneo alle ripartizioni ed agli uffici dell'Amministrazione Centrale".

23. Decreto del Direttore Generale n. 1071 del 24.07.2013 contenente l'istituzione della figura del "Responsabile della conservazione dei documenti informatici dell'Università degli Studi di Napoli Federico II".

24. Decreto Rettorale n. 3142 del 30.09.2013 recante l'Allegato 1 al Regolamento di Ateneo in materia di procedimento amministrativo e di diritto di accesso ai documenti.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A3. AREA ORGANIZZATIVA OMOGENEA E CARATTERISTICHE ORGANIZZATIVE

A3.1. Dati identificativi dell'Amministrazione

Denominazione dell'Amministrazione	Università degli Studi di Napoli Federico II
Codice Identificativo assegnato all'Amministrazione	
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Corso Umberto I, n.ro 40 – 80138 NAPOLI

A3.2. Caratterizzazione dell'Area Organizzativa Omogenea

Denominazione dell'Area Organizzativa Omogenea	Università degli Studi di Napoli Federico II
Codice Identificativo assegnato alla AOO	uni_na
Nominativo del Responsabile del Servizio per la tenuta del protocollo, dei documenti e dell'archivio	Dott.ssa Clelia Baldo
Nominativo del Responsabile del Servizio Informatico per la gestione del protocollo informatico, dei flussi documentali e dell'archiviazione elettronica	Prof. Guglielmo Tamburrini, Presidente del C.S.I.
Casella di posta elettronica certificata istituzionale dell'AOO	ateneo@pec.unina.it
Casella di posta elettronica interna dell'AOO	ateneo@unina.it
Indirizzo completo della sede principale della AOO a cui indirizzare cui indirizzare l'eventuale corrispondenza convenzionale	Corso Umberto I, n. 40 – 80138 NAPOLI
Data di istituzione della AOO	1.1.2007

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Articolazione della AOO in Uffici Organizzativi di Riferimento - UOR	Amministrazione Centrale, costituita da 9 Ripartizioni 26 Dipartimenti 26 Centri Interdipartimentali di Ricerca e di Servizio 11 Centri d'Ateneo 3 Centri museali 2 Centri d'Eccellenza 6 Centri Interuniversitari 12 Biblioteche di Area Altre strutture (Azienda Torre Lama, Orto botanico, Scuola specializzazione professioni legali)	
Articolazione della AOO in Unità Organizzative di registrazione di Protocollo - UOP	Il Responsabile dell'UOR definisce autonomamente le proprie UOP	Ciascuna UOP protocolla sia in ingresso che in uscita

A3.3. Organigramma del Protocollo Informatico

Di seguito, si riporta l'elenco delle UOR/UU definiti nell'organigramma del Protocollo Informatico, valido alla data di redazione del presente MdG. L'elenco aggiornato è pubblicato sul sito dell'eGovernment di Ateneo:

STRUTTURA	CODICE				
Amministrazione Centrale	1	1	0	0	0
Ripartizione Supporto Istituzionale	1	1	1	0	0
Segreteria Rettorato	1	1	1	1	0
Segreteria Direzione Generale	1	1	1	2	0
Ufficio Servizi Generali Amministrazione Centrale	1	1	1	3	0
Ufficio Organi Collegiali	1	1	1	4	0
Ufficio Servizi Generali Area Monte S. Angelo	1	1	1	11	0
Ripartizione Relazioni Studenti	1	1	2	0	0
Ufficio Dottorato, Assegni E Borse Di Studio	1	1	2	1	0
Segreteria Studenti Area Didattica Agraria	1	1	2	2	0
Segreteria Studenti Area Didattica Architettura	1	1	2	3	0
Segreteria Studenti Area Didattica Economia	1	1	2	4	0
Segreteria Studenti Area Didattica Giurisprudenza	1	1	2	5	0
Segreteria Studenti Area Didattica Ingegneria	1	1	2	6	0
Segreteria Studenti Area Didattica Studi Umanistici	1	1	2	7	0
Segreteria Studenti Area Didattica Medicina Veterinaria	1	1	2	8	0
Segreteria Studenti Area Didattica Scienze Mm.Ff.Nn.	1	1	2	9	0
Segreteria Studenti Area Didattica Scienze Politiche	1	1	2	10	0
Ufficio Esami Di Stato	1	1	2	11	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Segreteria Studenti Area Didattica Farmacia	1	1	2	12	0
Segreteria Studenti Area Didattica Medicina E Chirurgia	1	1	2	13	0
Segreteria Studenti Area Didattica Sociologia	1	1	2	14	0
Ufficio Scuole Di Specializzazione-Area Medica	1	1	2	15	0
Ufficio Relazioni Internazionali	1	1	2	16	0
Segreteria Studenti Area Didattica Scienze Biotecnologiche	1	1	2	17	0
Ufficio Scuole Di Specializzazione E Master - U.S.S.M.	1	1	2	18	0
Ufficio Tirocini Studenti	1	1	2	20	0
Ripartizione Personale Contrattualizzato, Pensioni, Aff.Spec.	1	1	3	0	0
Ufficio Personale Tecnico-Amministrativo	1	1	3	1	0
Ufficio Pensioni	1	1	3	2	0
Ufficio Affari Speciali Del Personale	1	1	3	4	0
Ufficio Relazioni Sindacali E Trattamento Accessorio	1	1	3	5	0
Ufficio Formazione	1	1	3	6	0
Ufficio Reclutamento Personale Contrattualizzato	1	1	3	7	0
Ufficio Assenze E Presenze Personale Contrattualizzato	1	1	3	8	0
Ripartizione Affari Generali, Professori E Ricercatori	1	1	4	0	0
Ufficio Affari Generali	1	1	4	2	0
Ufficio Statuto, Regolamenti E Organi Universitari	1	1	4	5	0
Ufficio Programmazione Universitaria E Affari Speciali	1	1	4	7	0
Ufficio Personale Docente E Ricercatore	1	1	4	8	0
Ufficio Scuola Delle Scienze Umane E Sociali	1	1	4	9	0
Ufficio Scuola Di Medicina E Chirurgia	1	1	4	10	0
Ufficio Scuola Politecnica E Delle Scienze Di Base	1	1	4	11	0
Ufficio Area Didattica Economia	1	1	4	12	0
Ripartizione Edilizia E Patrimonio	1	1	5	0	0
Ufficio Tecnico Per I Servizi Di Ingegneria Civile E Di Architettura	1	1	5	3	0
Ufficio Tecnico Per I Servizi Di Ingegneria Strutturale	1	1	5	4	0
Ufficio Tecnico Impianti Elettrici	1	1	5	7	0
Ufficio Tecnico Impianti Meccanici	1	1	5	8	0
Ufficio Patrimonio	1	1	5	10	0
Ufficio Di Supporto Della Programmazione Edilizia	1	1	5	13	0
Ripartizione Bilancio, Finanza E Sviluppo	1	1	7	0	0
Ufficio Contabilita' E Adempimenti Fiscali	1	1	7	1	0
Ufficio Stipendi	1	1	7	3	0
Ufficio Finanziamenti Per La Ricerca E Progetti Speciali	1	1	7	4	0
Ufficio Bilancio E Controllo	1	1	7	5	0
Ufficio Contabilita'	1	1	7	6	0
Ufficio Gestione Stralcio Residui Ex Polo St	1	1	7	7	0
Ufficio Gestione Stralcio Residui Ex Polo Stv	1	1	7	8	0
Ufficio Gestione Stralcio Residui Ex Polo Sus	1	1	7	9	0
Ufficio Gestione Proventi	1	1	7	10	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Ufficio Trasferimento Tecnologico Di Ateneo	1	1	7	11	0
Ripartizione Attivita' Contrattuale E Relazioni Con Il Pubblico	1	1	8	0	0
Ufficio Economato	1	1	8	2	0
Ufficio Per Le Relazioni Con Il Pubblico	1	1	8	4	0
Ufficio Gare E Contratti Per Servizi	1	1	8	5	0
Ufficio Gare E Contratti Per Lavori E Immobili	1	1	8	6	0
Ufficio Gare E Contratti Per Forniture	1	1	8	7	0
Ufficio Buoni Pasto,Centralino,Riprod. Xerografica	1	1	8	8	0
Ufficio Territoriale Sedi Decentrate	1	1	8	9	0
Ufficio Gestione Utenze Di Ateneo	1	1	8	10	0
Ripartizione Affari Legali,Procedure Elettorali,Valutazione	1	1	9	0	0
Ufficio Legale	1	1	9	1	0
Ufficio Per La Gestione Del Contenzioso Sul Lavoro	1	1	9	2	0
Ufficio Procedure Elettorali E Collaborazioni Studentesche	1	1	9	3	0
Ufficio Pianificazione Strategica E Valutazione	1	1	9	4	0
Ufficio Protocollo	1	1	9	5	0
Ufficio Archivio	1	1	9	6	0
Ripartizione Prevenzione,Protezione,Manutenzione	1	1	10	0	0
I Ufficio Prevenzione E Protezione	1	1	10	1	0
Ii Ufficio Prevenzione E Protezione	1	1	10	2	0
Iii Ufficio Prevenzione E Protezione	1	1	10	3	0
Ufficio Gestione Prevenzione Incendi	1	1	10	4	0
Ufficio Sorveglianza Sanitaria E Gestione Documentale	1	1	10	5	0
Ufficio Tecnico Area Centro 1	1	1	10	6	0
Ufficio Tecnico Area Centro 2	1	1	10	7	0
Ufficio Tecnico Area Centro 3	1	1	10	8	0
Ufficio Tecnico Area Centro 4	1	1	10	9	0
Ufficio Tecnico Monte S.Angelo	1	1	10	10	0
Ufficio Tecnico Fuorigrotta	1	1	10	11	0
Ufficio Tecnico Cappella Cangiani	1	1	10	12	0
Ufficio Tecnico Portici	1	1	10	13	0
Supporto Programmazione Manutenzione Ordinaria E Sicurezza	1	1	10	14	0
Centro Interdipartimentale Audiovisuale Per Lo Studio Della Cultura Popolare	1	7	1	0	0
Centro Interdipartimentale Vincenzo Arangio-Ruiz Di Studi Storici	1	7	2	0	0
Centro Interdipartimentale Di Ingegneria Per I Beni Culturali - C.I.Be.C.	1	7	3	0	0
Centro Interdipartimentale Di Servizio Metodologie Chimico-Fisiche	1	7	4	0	0
Centro Interdipartimentale Di Servizio Di Analisi Strumentale	1	7	5	0	0
Centro Interdipartimentale Di Ricerca Per L'analisi E La Sintesi Dei Segn	1	7	6	0	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Centro Interdipartimentale Di Ricerca Ambiente (Ciram)	1	7	7	0	0
Centro Interdipartimentale Di Ricerca Per Lo Studio Delle Tecniche Tradizi	1	7	8	0	0
Centro Interdipartimentale Di Ricerca Sui Biomateriali (Crib)	1	7	9	0	0
Centro Interdipartimentale Di Servizio Microscopia Elettronica (Cisme)	1	7	10	0	0
Centro Interdipartimentale Di Studi Italo-Spagnoli	1	7	11	0	0
Centro Interdipartimentale Di Studi Per La Magna Grecia	1	7	12	0	0
Centro Interdipartimentale Di Ricerca Per La Storia Comparata Delle Societ	1	7	13	0	0
Centro Interdipartimentale Di Servizio Di Radiologia Veterinaria	1	7	14	0	0
Centro Interdipartimentale Di Ricerca Laboratorio Di Urbanistica (Lupt)	1	7	15	0	0
Centro Interdipartimentale Di Ricerca Urban/Eco	1	7	16	0	0
Centro Interdipartimentale Di Servizi Per Analisi Geomineralogiche (Cisag)	1	7	17	0	0
Centro Interdipartimentale Di Ricerca In Urbanistica Alberto Calza Bini	1	7	18	0	0
Centro Interdipartimentale Di Ricerca Sperimentale Criacq-Centro Di Ricerc	1	7	19	0	0
Centro Interdipartimentale Di Ricerca Sperim. Iconografia Citta Europea	1	7	20	0	0
Centro Interdipartimentale Di Ricerca Sul Turismo	1	7	21	0	0
Centro Di Ateneo Per Orientamento, Formazione E Teledidattica Softel	1	7	22	0	0
Centro Linguistico Di Ateneo	1	7	23	0	0
Centro Musei Delle Scienze Naturali E Fisiche	1	7	24	0	0
Centro Interdipartimentale Di Ricerca Analisi E Prog. Urbana L.Pisciotti	1	7	25	0	0
Centro Servizi Veterinari	1	7	26	0	0
Centro Di Ricerca Per Studio Di Malattie Genetiche Ereditarie Ed Acquisite	1	7	27	0	0
Centro Di Ateneo Laboratorio Europeo Studio Malattie Indotte Da Alimenti	1	7	28	0	0
Centro Di Servizio Per La Radioprotezione E La Fisica Sanitaria	1	7	29	0	0
Centro di Ateneo Coord. Progetti Speciali, Innovazione Organizzativa (COINOR)	1	7	30	0	0
Centro Per La Qualita' Di Ateneo	1	7	31	0	0
Centro Interdipartimentale Di Ricerca Preclinica E Clinica Med. Sess.(Cirms)	1	7	32	0	0
Centro Di Ateneo Per I Servizi Informativi (C.S.I.)	1	7	33	0	0
Contact Center Csi	1	7	33	1	0
Basi Di Dati Csi	1	7	33	3	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Didattica E Segreteria Studenti Csi	1	7	33	4	0
E-Government Csi	1	7	33	5	0
Gestione Del Personale Csi	1	7	33	6	0
Gestione Finanziaria E Contabile Csi	1	7	33	7	0
Sviluppo Siti E Applicativi Csi	1	7	33	9	0
Qualita Csi	1	7	33	11	0
Reti Telematiche Csi	1	7	33	12	0
Supporto All'utenza - Csi	1	7	33	13	0
Sistemi Di Elaborazione E Microinformatica Csi	1	7	33	14	0
Metodologie,Tecnologie,Quality Assurance,Formazione Csi	1	7	33	15	0
Impianti Csi	1	7	33	16	0
Telefonia Csi	1	7	33	17	0
Segreteria Amministrativa Csi	1	7	33	52	0
Centro Di Eccellenza In Compositi Strutturali Applicazioni Innovative Scic	1	7	34	0	0
Centro Interdipartimentale Di Ricerca Farmacoeconomia, Farmacoutilizzazione	1	7	35	0	0
Centro Di Ateneo Innovazione E Sviluppo Dell'industria Alimentare (Caisial)	1	7	36	0	0
Centro Di Eccellenza Per L'innovazione Tecnologica In Chirurgia Itc	1	7	37	0	0
Centro Interdipartimentale Di Ricerca Scienze Immunologiche Di Base (Cisi)	1	7	38	0	0
Centro Interdipartimentale Di Ricerca Progetto Arch. E Urbanistico Contemp.	1	7	39	0	0
Centro Di Ricerca Interdipartimentale Risonanza Magnetica Nucleare (Cermanu	1	7	40	0	0
Centro Di Ateneo Per Le Biblioteche (Cab)	1	7	51	0	0
Centro Sinapsi - Servizi Per Inclusione Attiva E Partecipata Degli Studenti	1	7	52	0	0
Centro Museale Musa - Musei Delle Scienze Agrarie	1	7	53	0	0
Centro Di Servizi Metrologici Avanzati Cesma	1	7	54	0	0
Scuola Interuniversitaria Campana Di Specializzazione Insegnamento Sicsi	1	8	1	0	0
Sicsi Direzione	1	8	1	1	0
Sicsi Ateneo	1	8	1	2	0
Orto Botanico	1	8	2	0	0
Azienda Agraria Di Torre Lama	1	8	3	0	0
Centro Interuniversitario Di Studi In Economia E Finanza (Csef)	1	8	15	0	0
Centro Interuniversitario Di Ricerca Cirtibs(Tecn.Innovative Beni Strument.	1	8	16	0	0
Centro Interuniversitario Di Ricerca Bioetica (Cirb)	1	8	17	0	0
Centro Interuniversitario Di Ricerca Sui Peptidi Bioattivi (Cirpeb)	1	8	18	0	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Centro Interuniversitario Di Ricerca, Letteratura, Giornalismo(Cirleg)	1	8	19	0	0
Collegio Dei Revisori Dei Conti	1	8	20	0	0
Fondo Pensione Personale Docente,Tecnico E Amministrativo	1	8	21	0	0
Centro Interuniversitario Di Ricerca Su Azionamenti Per Trazione(Criat)	1	8	22	0	0
Centro Interuniversitario Di Ricerca Disturbi Comportam.Alimentare(Cirosdca)	1	8	23	0	0
Centro Interuniversitario Di Ricerca Storia Citta Campane Nel Medioevo	1	8	24	0	0
Centro Interuniversitario Di Ricerca Impatto Ambient. Sostanze Chim(Icreach)	1	8	25	0	0
Centro Interuniversitario Di Ricerca Mediterran.Cent.Advanced Stud.(Mecenas)	1	8	26	0	0
Comitato Etico Per Le Attivita' Biomediche	1	8	30	0	0
Scuola Di Specializzazione Per Le Professioni Legali	1	8	50	0	0
Biblioteca Area Economia	1	9	1	0	0
Biblioteca Area Giuridica	1	9	2	0	0
Biblioteca Area Scienze Sociali	1	9	3	0	0
Biblioteca Area Scienze Politiche	1	9	4	0	0
Biblioteca Area Medicina E Chirurgia	1	9	5	0	0
Biblioteca Area Agraria	1	9	6	0	0
Biblioteca Area Architettura	1	9	7	0	0
Biblioteca Area Farmacia	1	9	8	0	0
Biblioteca Area Ingegneria	1	9	9	0	0
Biblioteca Area Scienze Mmffnn	1	9	10	0	0
Biblioteca Area Medicina Veterinaria	1	9	11	0	0
Biblioteca Area Sociologia	1	9	12	0	0
Coord. Biblioteche Facolta' Di Giurisprudenza	1	9	16	0	0
Dipartimento Di Agraria	1	10	1	0	0
Dipartimento Di Architettura	1	10	2	0	0
Dipartimento Di Economia, Management, Istituzioni	1	10	3	0	0
Dipartimento Di Scienze Economiche E Statistiche	1	10	4	0	0
Dipartimento Di Farmacia	1	10	5	0	0
Dipartimento Di Giurisprudenza	1	10	6	0	0
Dipartimento Di Strutture Per Ingegneria E Architettura	1	10	7	0	0
Dipartimento Di Ingegneria Chimica,Materiali E Produzione Industriale	1	10	8	0	0
Dipartimento Di Ingegneria Civile,Edile E Ambientale	1	10	9	0	0
Dipartimento Di Ingegneria Elettrica E Delle Tecnologie Della Informazione	1	10	10	0	0
Dipartimento Di Ingegneria Industriale	1	10	11	0	0
Dipartimento Di Studi Umanistici	1	10	12	0	0

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	CODICE				
Dipartimento Di Scienze Mediche Traslazionali	1	10	13	0	0
Dipartimento di Neuroscienze, Scienze Riproduttive, Odontostomatologiche	1	10	14	0	0
Dipartimento Di Medicina Clinica E Chirurgia	1	10	15	0	0
Dipartimento Di Medicina Molecolare E Biotecnologie Mediche	1	10	16	0	0
Dipartimento Di Scienze Biomediche Avanzate	1	10	17	0	0
Dipartimento Di Sanita Pubblica	1	10	18	0	0
Dipartimento Di Medicina Veterinaria E Produzioni Animali	1	10	19	0	0
Dipartimento Di Biologia	1	10	20	0	0
Dipartimento Di Fisica	1	10	21	0	0
Dipartimento Di Matematica e Applicazioni Renato Caccioppoli	1	10	22	0	0
Dipartimento Di Scienze Chimiche	1	10	23	0	0
Dipartimento Di Scienze Della Terra, Ambiente E Risorse	1	10	24	0	0
Dipartimento Di Scienze Politiche	1	10	25	0	0
Dipartimento Di Scienze Sociali	1	10	26	0	0
Scuola Politecnica E Delle Scienze Di Base	1	11	0	0	0
Ufficio Area Didattica Ingegneria	1	11	1	0	0
Ufficio Area Didattica Architettura	1	11	2	0	0
Area Didattica Scienze Matematiche, Fisiche E Naturali	1	11	3	0	0
Scuola Medicina E Chirurgia	1	12	0	0	0
Area Didattica Medicina E Chirurgia	1	12	1	0	0
Area Supporto E Coord. Corsi Scienze Biotecnologiche	1	13	0	0	0
Scuola delle Scienze Umane e Sociali	1	14	0	0	0

A3.4. UOR e relativi codici di Registro emergenza

Di seguito, l'elenco delle UOR dotate di ufficio/postazione di protocollo, con i rispettivi codici di registro di emergenza.

STRUTTURA	REGISTRO DI EMERGENZA
Amministrazione Centrale	RE001
Centro Interdipartimentale Audiovisuale Per Lo Studio Della Cultura Popolare	RE701
Centro Interdipartimentale Vincenzo Arangio-Ruiz Di Studi Storici	RE702
Centro Interdipartimentale Di Ingegneria Per I Beni Culturali - C.I.Be.C.	RE703
Centro Interdipartimentale Di Servizio Metodologie Chimico-Fisiche	RE704
Centro Interdipartimentale Di Servizio Di Analisi Strumentale	RE705
Centro Interdipartimentale Di Ricerca Per L'analisi E La Sintesi Dei Segn	RE706
Centro Interdipartimentale Di Ricerca Ambiente (Ciram)	RE707
Centro Interdipartimentale Di Ricerca Per Lo Studio Delle Tecniche Tradizi	RE708

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	REGISTRO DI EMERGENZA
Centro Interdipartimentale Di Ricerca Sui Biomateriali (Crib)	RE709
Centro Interdipartimentale Di Servizio Microscopia Elettronica (Cisme)	RE710
Centro Interdipartimentale Di Studi Italo-Spagnoli	RE711
Centro Interdipartimentale Di Studi Per La Magna Grecia	RE712
Centro Interdipartimentale Di Ricerca Per La Storia Comparata Delle Societ	RE713
Centro Interdipartimentale Di Servizio Di Radiologia Veterinaria	RE714
Centro Interdipartimentale Di Ricerca Laboratorio Di Urbanistica (Lupt)	RE715
Centro Interdipartimentale Di Ricerca Urban/Eco	RE716
Centro Interdipartimentale Di Servizi Per Analisi Geomineralogiche (Cisag)	RE717
Centro Interdipartimentale Di Ricerca In Urbanistica Alberto Calza Bini	RE718
Centro Interdipartimentale Di Ricerca Sperimentale Criacq-Centro Di Ricerc	RE719
Centro Interdipartimentale Di Ricerca Sperim. Iconografia Citta Europea	RE720
Centro Interdipartimentale Di Ricerca Sul Turismo	RE721
Centro Di Ateneo Per Orientamento, Formazione E Teledidattica Softel	RE722
Centro Linguistico Di Ateneo	RE723
Centro Musei Delle Scienze Naturali E Fisiche	RE724
Centro Interdipartimentale Di Ricerca Analisi E Prog. Urbana L.Pisciotti	RE725
Centro Servizi Veterinari	RE726
Centro Di Ricerca Per Studio Di Malattie Genetiche Ereditarie Ed Acquisite	RE727
Centro Di Ateneo Laboratorio Europeo Studio Malattie Indotte Da Alimenti	RE728
Centro Di Servizio Per La Radioprotezione E La Fisica Sanitaria	RE729
Centro di Ateneo Coord. Progetti Speciali, Innovazione Organizzativa (COINOR)	RE730
Centro Per La Qualita' Di Ateneo	RE731
Centro Interdipartimentale Di Ricerca Preclinica E Clinica Med. Sess.(Cirms)	RE732
Centro Di Ateneo Per I Servizi Informativi (C.S.I.)	RE733
Centro Di Ateneo Per I Servizi Informativi (C.S.I.)	RE73D
Centro Di Eccellenza In Compositi Strutturali Applicazioni Innovative Scic	RE734
Centro Interdipartimentale Di Ricerca Farmacoeconomia, Farmacoutilizzazione	RE735
Centro Di Ateneo Innovazione E Sviluppo Dell'industria Alimentare (Caisial)	RE736
Centro Di Eccellenza Per L'innovazione Tecnologica In Chirurgia Itc	RE737

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	REGISTRO DI EMERGENZA
Centro Interdipartimentale Di Ricerca Scienze Immunologiche Di Base (Cisi)	RE738
Centro Interdipartimentale Di Ricerca Progetto Arch. E Urbanistico Contemp.	RE739
Centro Di Ricerca Interdipartimentale Risonanza Magnetica Nucleare (Cermanu	RE740
Centro Sinapsi - Servizi Per Inclusione Attiva E Partecipata Degli Studenti	RE752
Centro Di Servizi Metrologici Avanzati Cesma	RE754
Scuola Interuniversitaria Campana Di Specializzazione Insegnamento Sicsi	RE801
Sicsi Direzione	RE80B
Sicsi Ateneo	RE80L
Orto Botanico	RE802
Azienda Agraria Di Torre Lama	RE803
Centro Interuniversitario Di Studi In Economia E Finanza (Csef)	RE815
Centro Interuniversitario Di Ricerca Cirtibs (Tecn.Innovative Beni Strument.	RE816
Centro Interuniversitario Di Ricerca Sui Peptidi Bioattivi (Cirpeb)	RE818
Collegio Dei Revisori Dei Conti	RE820
Fondo Pensione Personale Docente, Tecnico E Amministrativo	RE821
Scuola Di Specializzazione Per Le Professioni Legali	RE850
Biblioteca Area Economia	RE901
Biblioteca Area Giuridica	RE902
Biblioteca Area Umanistica	RE903
Biblioteca Area Scienze Politiche	RE904
Biblioteca Area Medicina E Chirurgia	RE905
Biblioteca Area Agraria	RE906
Biblioteca Area Architettura	RE907
Biblioteca Area Farmacia	RE908
Biblioteca Area Ingegneria	RE909
Biblioteca Area Scienze Mmffnn	RE910
Biblioteca Area Medicina Veterinaria	RE911
Biblioteca Area Sociologia	RE912
Coord. Biblioteche Facolta' Di Giurisprudenza	RE916
Dipartimento Di Agraria	REA01
Dipartimento Di Architettura	REA02
Dipartimento Di Economia, Management, Istituzioni	REA03
Dipartimento Di Scienze Economiche E Statistiche	REA04
Dipartimento Di Farmacia	REA05

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

STRUTTURA	REGISTRO DI EMERGENZA
Dipartimento Di Giurisprudenza	REA06
Dipartimento Di Strutture Per Ingegneria E Architettura	REA07
Dipartimento Di Ingegneria Chimica, Materiali E Produzione Industriale	REA08
Dipartimento Di Ingegneria Civile, Edile E Ambientale	REA09
Dipartimento Di Ingegneria Elettrica E Delle Tecnologie Della Informazione	REA10
Dipartimento Di Ingegneria Industriale	REA11
Dipartimento Di Studi Umanistici	REA12
Dipartimento Di Scienze Mediche Traslazionali	REA13
Dipartimento Di Neuroscienze,Scienze Riproduttive, Odontostomatologiche	REA14
Dipartimento Di Medicina Clinica E Chirurgia	REA15
Dipartimento Di Medicina Molecolare E Biotecnologie Mediche	REA16
Dipartimento Di Scienze Biomediche Avanzate	REA17
Dipartimento Di Sanita Pubblica	REA18
Dipartimento Di Medicina Veterinaria E Produzioni Animali	REA19
Dipartimento Di Biologia	REA20
Dipartimento Di Fisica	REA21
Dipartimento Di Matematica E Applicazioni Renato Caccioppoli	REA22
Dipartimento Di Scienze Chimiche	REA23
Dipartimento Di Scienze Della Terra, Ambiente E Risorse	REA24
Dipartimento Di Scienze Politiche	REA25
Dipartimento Di Scienze Sociali	REA26
Scuola Politecnica E Delle Scienze Di Base	REB00
Scuola Medicina E Chirurgia	REC00
Area Supporto E Coord. Corsi Scienze Biotecnologiche	RED00
Scuola delle Scienze Umane e Sociali	REE00

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A4. ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO DI COORDINAMENTO DEL PROTOCOLLO INFORMATICO

U.P.T.A. **D.D. 3 del 7.1.2009**

IL DIRETTORE AMMINISTRATIVO

PREMESSO che il D.P.R. 28 dicembre 2000, n. 445 e successive modifiche ed integrazioni "Testo unico delle disposizioni legislative in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione dei flussi documentali coordinata con la gestione dei procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare i supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

VISTO in particolare l'art. 61 del succitato D.P.R. 445/2000 che – tra l'altro – prevede, presso ciascuna amministrazione, l'istituzione di un Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate, attribuendo a tale Servizio, al comma 3, lo svolgimento di compiti definiti;

VISTO il D. M. 14 ottobre 2003 recante "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi", nel quale sono indicati gli adempimenti delle amministrazioni relativamente al protocollo informatico ed alla gestione dei procedimenti amministrativi con tecnologie informatiche;

VISTO il D.Lgs. 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" nel quale, tra l'altro, si forniscono alle pubbliche amministrazioni le direttive per un uso a norma delle tecnologie dell'informazione e della comunicazione per consentire: l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni ed una completa gestione informatica dei procedimenti amministrativi e dei fascicoli in cui la pubblica amministrazione titolare del procedimento può raccogliere gli atti, i documenti ed i dati del procedimento medesimo da chiunque formati;

TENUTO CONTO che nel corso del 2005 l'Università degli Studi di Napoli Federico II ha avviato la realizzazione del progetto "Protocollo Informatico" ed ha successivamente acquisito la soluzione tecnologica implementata dalla Regione Campania "E-Grammata" attraverso la formula del riuso, a seguito di

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

autorizzazione conferita dalla Regione Campania con Nota N. Prot. 2006.0228968 del 13.03.2006 e successiva stipula del Protocollo di Intesa tra i due Enti, autorizzato dal Consiglio di Amministrazione con delibera n. 19 del 31 marzo 2006 e sottoscritto tra le parti in data 10 maggio 2006;

TENUTO CONTO che, ai fini della gestione documentale, vista la forte coesione interna ed il coordinamento tra le strutture che costituiscono l'Ateneo, l'Università degli Studi di Napoli Federico II si è configurata come unica Area Organizzativa Omogenea di cui fanno parte l'Amministrazione Centrale, i Poli, le Facoltà, i Dipartimenti, i Centri di Ateneo, i Centri interdipartimentali di Servizio e di Ricerca, le Biblioteche e tutte le restanti strutture dotate di autonomia economico-gestionale (nel seguito denominate UOR – Unità Organizzative Responsabili) e che, in virtù della scelta organizzativa sopra citata, è stato inoltre istituito, in data 1 gennaio 2007, il "Protocollo Generale dell'Università degli Studi di Napoli Federico II" (unico, per tutte le strutture dell'Ateneo), con il contestuale avvio dell'esercizio del nuovo Sistema del Protocollo Informatico;

TENUTO CONTO che, con particolare riferimento alla gestione del protocollo, dei flussi documentali e degli archivi, ciascuna UOR provvede, in autonomia organizzativa ed operativa e nel rispetto della normativa vigente, dei regolamenti e delle disposizioni interni dell'Ateneo, alla registrazione (eventualmente anche su registro di emergenza), alla classificazione, alla assegnazione, all'annullamento delle registrazioni di protocollo, alla conservazione dei documenti di propria competenza e, nel caso dell'Amministrazione Centrale e dei Poli, alla gestione degli archivi;

CONSIDERATO che l'innovazione dei processi e dei servizi basata sull'utilizzo a norma e la diffusione delle tecnologie dell'informazione e della comunicazione è determinata e pianificata dagli organi di vertice dell'Ateneo che si avvalgono, tra l'altro, della consulenza ed il supporto del Centro di Ateneo per i Servizi Informativi (C.S.I.), con particolare riguardo all'area tecnica "e-Government", a ciò istituita con D.D. n. 1855 del 29 dicembre 2006;

CONSIDERATO che per proseguire il percorso di adeguamento dell'Ateneo con quanto stabilito dalla normativa vigente in materia di amministrazione digitale e di gestione informatica della documentazione amministrativa è necessario proporre, pianificare ed attuare la realizzazione di soluzioni integrate sotto il profilo tecnologico, metodologico e di processo, coerenti con le politiche di e-Government dell'Ateneo suesposte;

CONSIDERATO che il perseguimento degli obiettivi sopraindicati richiede la cooperazione forte e coordinata con tutte le strutture ed uffici dell'Ateneo, affinché, pur nell'ambito delle specifiche responsabilità di tipo organizzativo ed operativo, sia possibile il loro necessario coinvolgimento partecipativo nella

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

definizione ed applicazione di regole e prassi e nell'attuazione delle soluzioni innovative previste dal piano dell'e-Government;

SENTITO il Presidente del Centro Servizi Informativi d'Ateneo (C.S.I.);

DECRETA

ART. 1) È istituito, ai sensi all'art. 61 del succitato D.P.R. 445/2000, il "Servizio di Coordinamento del Protocollo Informatico" per la gestione informatica dei documenti, dei flussi documentali e degli archivi

ART. 2) Al "Servizio di Coordinamento del Protocollo Informatico" vengono attribuite le seguenti specifiche competenze:

- Interviene su tutte le U.O.R. dell'Ateneo di cui in premessa, nel rispetto della autonomia operativa di ciascuna struttura, con funzione di coordinamento, monitoraggio e controllo in merito agli adempimenti connessi con la procedura del protocollo informatico e di gestione dei flussi documentali;
- Garantisce che il sistema informatico consenta lo svolgimento delle operazioni di registrazione e di segnatura di protocollo in ottemperanza con quanto stabilito dalla legislazione vigente in materia;
- Attiva il Centro Servizi Informativi d'Ateneo (C.S.I.) affinché le funzionalità del sistema, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile, coerentemente con livelli di servizio preventivamente concordati e, comunque entro le ventiquattro ore dal blocco delle attività;
- Stabilisce con il C.S.I. le procedure per la corretta produzione e conservazione del registro giornaliero di protocollo e per la conservazione delle copie di salvataggio delle informazioni del sistema e vigila sull'osservanza di quanto concordato;
- Definisce i profili di abilitazione (ruoli) per l'accesso alle funzioni ed ai dati del sistema di Protocollo Informatico che i responsabili di U.O.R. attribuiscono ai propri incaricati;
- Propone i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, e, più in generale, dei protocolli diversi dal protocollo informatico;
- Fornisce consulenza alle strutture in materia per quanto attiene alla attuazione delle politiche di gestione informatica dei documenti, dei fascicoli ed dei flussi documentali;
- Predispone lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo e ne cura l'aggiornamento;
- Provvede alla pubblicazione del manuale anche per via telematica;
- Predispone il piano per la sicurezza informatica relativo alla protezione della integrità, della riservatezza e della disponibilità dei documenti e delle informazioni trattate nell'ambito del sistema di Protocollo

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Informatico e di gestione dei flussi documentali, d'intesa con il C.S.I. ed il titolare dei trattamenti dei dati di cui al dlgs. n. 196/2003 "Codice in materia di protezione dei dati personali";

- Garantisce l'adeguatezza degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e di gestione informatica degli archivi elettronici;
- Aggiorna il Titolario di classificazione, sulla base delle indicazioni fornite dalle U.O.R.;
- Cura, d'intesa con i responsabili degli uffici preposti alla gestione degli archivi, la definizione dei requisiti del sistema di conservazione a norma dei documenti cartacei.

ART. 3) Il Servizio è istituito nell'ambito dell'Area Tecnica "e-Government" del C.S.I. e si avvale della collaborazione delle Aree Tecniche del C.S.I. e dell'Ufficio Protocollo ed Archivio dell'Amministrazione Centrale e degli Uffici Protocollo dei Poli.

ART. 4) Responsabile del servizio "Servizio di Coordinamento del Protocollo Informatico" è nominata la dott.ssa Clelia BALDO, cat EP, pos. econ. EP2, area tecnica, tecnico-scientifica ed elaborazione dati, Direttore dell'Area Tecnica "e-Government" del C.S.I., che risponderà direttamente al Direttore Amministrativo.

IL DIRETTORE AMMINISTRATIVO

Dott.ssa Maria Luigia LIGUORI

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A5. I TITOLARI DI FIRMA DIGITALE

L'elenco dei titolari di firma è custodito e tenuto dagli Incaricati_firma nominati dall'Amministrazione per svolgere le funzioni di identificazione dei titolari, di registrazione, emissione certificati e consegna del kit di firma agli interessati. Le informazioni relative alla anagrafica completa e allo stato (scaduto/rinnovato/sospeso/revocato) dei certificati è comunque disponibile presso le Certification Authority fornitrici dei dispositivi di firma dell'Università (IT Telecom S.p.A. e ARUBA PEC S.p.A.). Inoltre, periodicamente le due CA inviano al C.S.I. un flusso con i dati anagrafici aggiornati sui titolari e rispettivi certificati e il CSI provvede quindi al popolamento di una base dati interrogabile mediante l'applicazione Web denominata "CerDi", il cui accesso è protetto mediante controllo di autenticazione ed abilitazione.

Di seguito si riporta, in modo sintetico, l'elenco dei ruoli dei titolari di kit di firma digitale:

RUOLO
RETTORE
DIRETTORE GENERALE
PRORETTORE
DIRIGENTI
RESPONSABILI UOR
CAPO UFFICIO ORGANI COLLEGIALI
CAPO UFFICIO URP
RESPONSABILI TECNICI SERVIZIO UNINAPEC
AREA EGOVERNMENT DEL CSI
DOCENTI (Utilizzatori Verbale digitale)
RUP

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A6. PIANO FORMATIVO PER IL PERSONALE DELL'AMMINISTRAZIONE PER L'AVVIO DEL SISTEMA

Di seguito, si descrive l'organizzazione dei corsi di addestramento al personale dell'Ateneo all'utilizzo del PdP. Tali corsi sono stati erogati, fatta eccezione del modulo MSYS (erogato dal Fornitore del PdP), da unità di personale interno afferente all'area tecnica eGovernment del CSI sia in fase di avviamento che in modo periodico, al fine di aggiornare gli addetti al PdP alle novità regolamentari e tecnologiche del sistema.

A6.1. I moduli formativi

In relazione alla formazione utenti, sono stati erogati i seguenti corsi:

Modulo INTRODUTTIVO COMUNE (MIC): seminario sui principali concetti dell'Amministrazione Digitale, PEC, Firma Digitale, sull'architettura del servizio di Protocollo.
Durata: 2 hh.
Partecipanti: Responsabili (di struttura), Responsabili dei Servizi di Protocollo, Amministratori di sistema.

Modulo ARCHITETTURA PROTOCOLLO (MAP): seminario sull'architettura, sull'organizzazione del servizio di Protocollo e sul menù e funzioni di E-Grammata, con particolare riguardo alle funzionalità di ricerca, al concetto di interoperabilità ed al processo di sigla dei documenti informatici.
Durata: 2 hh.
Partecipanti: Responsabili (di struttura) e Responsabili dei Servizi di Protocollo.

Modulo FORMAZIONE PROTOCOLLISTA (MFP): corso su tematiche funzionali e applicative, assegnate al ruolo di Protocollista;
Durata: una giornata (8 hh.)
Partecipanti: Protocollisti.

Modulo DOCUMENTO INFORMATICO (MDI): corso su tematiche funzionali e applicative per la gestione dei documenti informatici e dell'iter amministrativo;
Durata: 2 mezze giornate (4 hh. + 4 hh.)
Partecipanti: Responsabili dei Servizi di Protocollo, Protocollisti.

Modulo PROTOCOLLISTA AMMINISTRAZIONE CENTRALE (MAC): corso focalizzato sulla operatività del protocollista base addetto alla segnatura massiva dei documenti dell'Amministrazione Centrale;

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Durata: mezza giornata (4 hh.)
Partecipanti: Responsabile del Servizio di Protocollo dell'Amministrazione Centrale e Protocollista in servizio presso l'Ufficio di Protocollo dell'Amministrazione Centrale.

Modulo AMMINISTRATORE DI SISTEMA (MSYS): su tematiche di amministrazione sistemistica dell'applicazione, del data base e dei dispositivi periferici.
Durata: 1 giorno
Partecipanti: Amministratori di sistema.

Di seguito, una tabella di sintesi:

Modulo Corso	Codice Corso	Numero giornate	Numero Edizioni
Modulo INTRODUTTIVO COMUNE	MIC	0,25	5
Modulo FORMAZIONE RESPONSABILE	MAP	0,25	5
Modulo FORMAZIONE PROTOCOLLISTA	MFB	2	5
Modulo DOCUMENTO INFORMATICO	MDI	(2 x 0,5)	5
Modulo PROTOCOLLAZIONE AMMINISTRAZIONE CENTRALE	MAC	0,5	2
Modulo AMMINISTRATORE DI SISTEMA	MSYS	1	1

A6.2. I profili dei fruitori dei corsi

Obiettivo dei corsi è quello di fornire al personale, individuato dall'ente, addetto alla protocollazione nei diversi punti di protocollazione decentrata, all'utilizzo delle funzionalità del nuovo sistema del protocollo.
Il corso è orientato a utenti caratterizzati da diversi profili; tali profili sono identificati tramite set di caratteristiche e abilitazioni a funzioni dell'applicativo.

RESPONSABILE DI STRUTTURA/DI SIGLA: è il responsabile di un processo di lavoro, cui è demandata la gestione della sigla e della assegnazione delle pratiche protocollate. Si identifica col responsabile di una struttura o suo delegato. Si occupa della registrazione di protocollo particolare.

Ruoli: Responsabili di struttura, Responsabili del servizio di protocollo, Funzionari di segreteria con delega di sigla, oppure addetti al protocollo particolare.

RESPONSABILE DEL SERVIZIO DI PROTOCOLLO: è il responsabile del servizio di protocollo di una struttura. Si occupa del coordinamento delle attività dei protocollisti, gestisce il registro di emergenza, l'assegnazione delle pratiche per il completamento della registrazione di protocollo, l'annullamento o il differimento della registrazione di protocollo.
Ruoli: Responsabili del servizio di protocollo, Responsabile Ufficio Protocollo ed Archivio dell'Amministrazione Centrale.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

PROTOCOLLISTA: si occupa della protocollazione, in ingresso e uscita, dei documenti, su formato cartaceo ed informatico. Ha accesso alle più comuni funzioni e strumenti di protocollazione, tra cui, eventualmente, le funzionalità di Posta Elettronica Certificata/Istituzionale. Si occupa inoltre di registrare lo smistamento dei documenti, e delle eventuali copie, alle Unità funzionali dipendenti o ai singoli collaboratori. Può svolgere funzioni di classificazione e fascicolazione, secondo l'organizzazione specifica dell'unità di lavoro in cui è inserito.
Se è anche addetto alla gestione dei documenti informatici, accede agli strumenti di interoperabilità e Posta Elettronica Certificata/Istituzionale.
Tra gli operatori di protocollo base, vanno inclusi i protocollisti dell'Ufficio di Protocollo dell'Amministrazione Centrale, addetti alla segnatura ed acquisizione massiva.

Ruoli: Responsabili del servizio di protocollo, Responsabile Ufficio Protocollo ed Archivio dell'Amministrazione Centrale, Operatori di Protocollo, Addetti di segreteria del Direttore Generale e del Rettore.

AMMINISTRATORE DI SISTEMA: è responsabile della amministrazione dei sistemi hardware e degli ambienti software. Amministra le politiche di salvataggio e storicizzazione dei dati, garantisce l'attuazione dei meccanismi informatici previsti nel Piano della Sicurezza. Aggiorna il sistema di autorizzazione degli utenti. Garantisce l'adeguatezza, la disponibilità e la piena operatività delle postazioni di protocollazione, complete delle rispettive periferiche (scanner ed etichettatrice).

Ruoli: Tecnici applicativi, Sistemisti, Data Base Administrator, Tecnici per la manutenzione dei PdL.

A6.3. I Percorsi formativi

Profilo	Codice Corso	Numero giornate	Totale giornate
RESPONSABILE	MIC	0,25	**2 x (0,25)**
	MAP	0,25	
RESPONSABILE SERVIZIO PROTOCOLLO	MIC	0,25	**2,25**
	MFP	1	
	MDI	2 x 0,5	
PROTOCOLLISTA	*MIC* (*)	*0,25*	**1,5** + (0,25) + (1)
	MFP	1,5	
	MDI (*)	*2 x 0,5*	
PROTOCOLLISTA A. C.	*MIC* (*)	*0,25*	**1,5** + (0,25) + (1)
	MFP	1	
	MDI (*)	*2 x 0,5*	
	MAC	0,5	
AMMINITRATORE DI SISTEMA	*MIC* (*)	0,25	**1** + (0,25)
	MSYS	1	

(*) = Il modulo è da ritenersi non obbligatorio, per lo specificato profilo.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A6.4. Dettaglio del contenuto dei corsi

Di seguito si fornisce il programma dei corsi :

Modulo INTRODUTTIVO COMUNE (MIC)

DUE ORE	• L'Amministrazione Digitale o Alcuni richiami normativi in materia di amministrazione digitale o Gli strumenti per l'e-government: o Il Protocollo Informatico o La Posta Elettronica Certificata o La Firma Digitale • Architettura del servizio di Protocollo Informatico, di PEC e di Firma Digitale

Modulo ARCHITETTURA PROTOCOLLO (MAP)

DUE ORE	- Introduzione all'applicativo E-Grammata - L'accesso all'applicazione. - Presentazione delle funzionalità del sistema: il menù e la sua organizzazione in gruppi di funzioni - Navigazione del programma - Standard Struttura delle mappe - Cenni su Struttura Organizzativa e Titolario - La ricerca dei documenti protocollati - Il processo di sigla - Il protocollo particolare

Modulo PROTOCOLLAZIONE AMMINISTRAZIONE CENTRALE (MAC)

MEZZA GIORNATA UNICA	- Il procedimento di acquisizione massiva dei documenti da protocollare, con segnatura - Assegnazione e completamento delle registrazioni - Gestione delle anomalie

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Modulo FORMAZIONE PROTOCOLLISTA (MFP)

PRIMA GIORNATA	Introduzione all'applicativo E-Grammata L'accesso all'applicazione. Presentazione delle funzionalità del sistema: il menù e la sua organizzazione in gruppi di funzioni Navigazione del programma Standard Struttura delle mappe Cenni su Struttura Organizzativa e Titolario Protocollo Generale Funzioni speciali: Modifica del primo assegnatario Modifica dati registrazione Annullamento registrazione Modifica classificazione Gestione degli atti di autorizzazione alla protocollazione differita Gestione degli atti di autorizzazione all'annullamento di registrazione Annullamento dati di registrazione Annullamento copia Ripristino registrazione annullata Funzioni di scansione massiva per le strutture
	Esercitazioni
SECONA MEZZA GIORNATA	- Riepilogo concetti della prima giornata - Protocollazione differita - Client di emergenza
	Esercitazioni

Modulo DOCUMENTO INFORMATICO ED ITER DOCUMENTALE(MDI)

PRIMA MEZZA GIORNATA	- Protocollo generale: - Interoperabilità - Casella e-mail su dominio unina e su pec.unina.it - Il processo di sigla - Protocollazione di documenti informatici di provenienza valida, non interoperabili

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

SECONDA MEZZA GIORNATA	- Iter documentale: - Invio ad altri uffici - Archivio Appoggio - Lista Lavoro Documenti - Gestione Copie
	Esercitazioni

Modulo per AMMINISTRATORI di SISTEMA

GIORNATA UNICA	**Amministrazione del sistema** - Architettura tecnologica: le componenti che entrano in gioco nelle varie funzionalità - Procedure di start-up / stop dell'applicazione E-Grammata - Informazioni in relazione al log - Integrazione LDAP: configurazione e requisiti - Integrazione Posta certificata / modulo Interoperabilità - Integrazioni modulo firma digitale: configurazioni, installazioni e requisiti - Modulo di scansione interattiva e massiva: configurazioni, installazioni e requisiti - Moduli di stampa interattiva e schedulata: configurazioni, installazioni e requisiti - I Web Services: come sono stati sviluppati, come installarli, come richiamarli - Struttura della banca dati - L'utente MMASTER - Lo schema Oracle - Il Cryptoserver e la funzionalità per l'installazione e l'aggiornamento dei certificati qualificati - I parametri di configurazione di E-Grammata - Procedure di gestione del sistema - La stampa giornaliera ed annuale del registro di protocollo **Servizio di manutenzione** - Installazione nuove release - Descrizione CVT – Parametri

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A7. PIANO DI ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

Di seguito si riportano gli obiettivi e le fasi in cui si è articolato il piano di diffusione del PdP all'intero Ateneo.

Obiettivo 0: Istituzione del Protocollo Generale ed avvio del sistema presso l'Amministrazione centrale e le strutture pilota.

Il sistema, acquisito in riuso dalla Regione Campania e personalizzato secondo i requisiti specifici dell'Ateneo, è stato avviato presso lì Amministrazione Centrale, i Poli, il C.S.I. e due dipartimenti pilota.
Fase 1 – Ricognizione della situazione. Analisi e individuazione della nuova architettura di servizio

Fase 2 – Acquisizione, personalizzazione e configurazione dell'applicazione informatica.

Fase 3 – Formazione utenti pilota ed avvio dell'esercizio.

Obiettivo 1: Unificazione dei registri di protocollo delle strutture decentrate nel Protocollo Generale di Ateneo.

Una completa gestione elettronica ed integrata dei flussi documentali dell'Ateneo non può prescindere dall'utilizzo condiviso di un sistema unico ed integrato per:

- la registrazione dei dati,
- il reperimento delle informazioni,
- la gestione del flusso di lavoro,
- l'interoperabilità interna e con enti esterni, basata sull'utilizzo di regole codificate e di standard tecnologici.

Tale obiettivo si è stato quindi realizzato mediante la diffusione del Protocollo informatico a tutte le restanti strutture dell'Ateneo (Facoltà, Dipartimenti e Centri).

Fase 1 – Acquisizione e distribuzione apparecchiature per attrezzare le postazioni di lavoro.

Fase 2 – Formazione degli utenti.

Fase 3 – Avvio progressivo delle strutture secondo una pianificazione di dettaglio.

Obiettivo 2 - Riduzione del flusso cartaceo (per i documenti in ingresso alla

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Amministrazione Centrale) tra la Direzione Amministrativa e gli Uffici dell'Amministrazione Centrale assegnatari.

Fase 1 - Ampliamento delle funzionalità del Protocollo Informatico, in modo da consentire la gestione del workflow dell'iter documentale.

Sono state stabilite regole ed è stata configurata l'applicazione di Protocollo Informatico in modo tale da consentire la gestione dei vari stati di lavorazione di un documento: dalla sua registrazione, alla sigla ed assegnazione da parte del Direttore Generale o del Responsabile di sigla preposto, alla presa in carico da parte di ciascun assegnatario o, in alternativa, alla restituzione del documento stesso da parte del Capo Ufficio al Responsabile di sigla, per la successiva ri-assegnazione del documento.

Il modello proposto, in totale coerenza con l'attuale processo di sigla, si basa sull'implementazione delle seguenti regole:

1. Nel caso di protocollazioni interne che provengono da strutture di I livello (UOR) dotate di Protocollo Informatico, l'UOR origine deve impostare come destinatario non l'Ufficio, bensì la Direzione Amministrativa, che rappresenta la UOR nel suo complesso.
2. La Direzione Generale sigla ed assegna il documento ricevuto, oppure, in alternativa, smista il documento ad un Responsabile di sigla (Dirigente di Ripartizione). Possono risultare assegnatari uno o più Uffici.
3. Ciascun Ufficio assegnatario prende in carico la pratica soltanto se è di propria competenza e se la pratica risulta siglata dal Responsabile di sigla. Se la pratica non è di propria competenza, la restituisce al Responsabile di sigla per la successiva ri-assegnazione. Se, invece, la pratica non è siglata (per esempio, la UOR ha inoltrato il documento direttamente all'Ufficio), provvede ad inviarla in Direzione Generale.

Fase 2 - Diffusione del Protocollo Informatico agli Uffici dell'Amministrazione Centrale.

Coerentemente con quanto definito nel punto precedente, al fine di consentire il reperimento dei documenti protocollati e la tempestiva presa in carico delle pratiche da parte degli Uffici, è stato quindi consentito l'accesso al sistema di Protocollo Informatico anche ai Capi Ufficio ed a loro incaricati.

Pertanto, è stato definito nel sistema il nuovo profilo "Ufficio", associato a nuovi utenti: più in dettaglio, per ciascun Ufficio sarà definito un utente le cui credenziali sono quelle della posta elettronica del Capo Ufficio ed un utente di ruolo, le cui credenziali sono quelle della posta elettronica dell'Ufficio.

Ciascun Capo Ufficio è stato quindi messo in grado di accedere alla propria lista lavoro, visualizzare tutti i documenti, prenderli in carico, smistarli alla Direzione Generale, nel caso di erronea trasmissione da parte della UOR mittente. Nel caso di errata

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

assegnazione, il Capo Ufficio trasmette il documento alla Direzione Generale. Il processo di ri-assegnazione si completa ad opera dell'Ufficio di Protocollo che provvede allo smistamento del documento cartaceo al nuovo assegnatario e, mediante apposita funzionalità informatica, al cambio dell'assegnatario.

In prima applicazione, il processo cartaceo di sigla e di smistamento non viene modificato, salvo che per la riduzione della carta, visto che l'originale cartaceo viene inviato solo al primo assegnatario. Un sostanziale miglioramento dei tempi e l'eliminazione – salvo casi specifici in cui viene inviata dal mittente interno anche il documento originale – del flusso cartaceo è stato raggiunto con l'attuazione della fase successiva.

Fase 3 - Organizzazione del processo di sigla presso la Direzione Amministrativa e le Ripartizioni.

Tale fase ha previsto la definizione di un nuovo profilo di utenza, quello del "Responsabile di sigla". In particolare, sono stati definiti più Responsabili di sigla, ciascuno in corrispondenza delle seguenti unità organizzative: la Direzione Generale e le Ripartizioni dell'Amministrazione Centrale.

Il Direttore Generale (oppure, un suo incaricato), sulla base dei documenti (cartacei) provenienti da strutture dotate di Protocollo Informatico - e quindi dotati di codice di protocollo del tipo "PGxxxxxxx" - accede alla lista di lavoro dell'Amministrazione Centrale e provvede a prendere in carico i documenti e ad inviarli agli Uffici competenti.

I Capi Ufficio destinatari prendono in carico elettronicamente solo i documenti loro assegnati che provengono dal Responsabile di sigla (elemento che si evince dalla lista dei movimenti di ciascun documento). Nel caso in cui il documento sia stato inviato dalla UOR mittente direttamente all'Ufficio, il Capo Ufficio smista elettronicamente il documento, senza prenderlo in carico, alla Direzione Amministrativa e contestualmente spedisce in Direzione anche il documento cartaceo.

Se il documento, correttamente siglato, non è di competenza dell'Ufficio, il Capo Ufficio lo restituisce al Responsabile di sigla il quale può quindi annullare la copia e eventualmente, procedere con l'assegnazione ad un diverso Ufficio.

Il I assegnatario è l'unico destinatario anche del documento cartaceo origine. Pertanto, è l'unico assegnatario che, in caso di recapito diretto oppure di restituzione, dovrà trasmettere al Responsabile di sigla anche il documento cartaceo.

Il sistema traccia tutti i movimenti eseguiti dai vari soggetti sulla registrazione di protocollo, completi di data ed ora, ragion per cui il Responsabile di sigla può monitorare la effettiva presa in carico dei documenti da parte dei vari Uffici. Inoltre, è disponibile la stampa dei movimenti di assegnazione e smistamento effettuati dalla

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

postazione del Responsabiledi sigla, sotto forma di un "Rapportino di consegna".

Tale soluzione è stata successivamente estesa ai Poli, fino alla cessazione di tali strutture (31.12.2012).

Obiettivo 3 - Riduzione del flusso cartaceo tra le strutture dell'Ateneo.

Fase 1 - Eliminazione della minuta. Il documento originale, dopo la registrazione di protocollo, viene custodito dal mittente (solo flusso interno).

Al fine di ridurre il consumo di carta, solo per i flussi interni tra strutture dotate di Protocollo Informatico, si è stabilito che ciascun Responsabile del procedimento produca il documento in un'unica copia. Il documento cartaceo, dopo la sigla e la registrazione di protocollo, se destinato a una struttura interna dotata di Protocollo Informatico, viene dunque restituito dall'Ufficio di protocollo al mittente. Il destinatario, infatti, riceve la versione elettronica del documento (completa di segnatura di protocollo) e può:

a) nel caso dell'Amministrazione Centrale, avviare il processo di sigla e di assegnazione,
b) nel caso di strutture semplici, prendere in carico il documento (da parte dell'Ufficio di Protocollo) e procedere allo smistamento interno della pratica.

È opportuno evidenziare che il raggiungimento dell'obiettivo 5 è stato propedeutico all'implementazione di tale fase.

Fase 2 - Diffusione della firma digitale ai Responsabili delle strutture.

I documenti formati dalle strutture mittenti possono essere sottoscritti con firma digitale del Responsabile della struttura e quindi protocollati.

L'implementazione del timbro digitale (basato su codifica PDF417) consente di includere nella versione a stampa del documento in un codice grafico bidimensionale nel quale sono riportate, crittograficamente, informazioni riguardanti la segnatura di protocollo ed i dati relativi al certificato qualificato del sottoscrittore utilizzato per la firma digitale, consentendo quindi la successiva verifica di autenticità del documento informatico.

Obiettivo 4 – Snellimento del carico di lavoro dell'Ufficio di Protocollo dell'Amministrazione Centrale.

Nel medio termine, si potrà realizzare un'apposita nuova funzione informatica che consenta – sempre per le sole registrazioni di protocollo interne all'Ateneo – la predisposizione da parte di ciascun Capo Ufficio dei dati di registrazione di protocollo in uscita dall'Amministrazione Centrale (o, in seguito, dai Poli). In tal caso, i documenti

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

allegati alla richiesta di protocollo dovranno essere informatici ed in formato pdf.

Il Responsabile di sigla potrà quindi visualizzare le pratiche in attesa di registrazione di protocollo, vistarle (contestualmente consentendone l'automatica registrazione), eventualmente apponendo preventivamente la propria firma digitale, oppure, restituirle all'Ufficio responsabile complete delle note, delle correzioni e delle osservazioni del caso.

Il documento protocollato sarà quindi subito disponibile nelle liste di lavoro delle strutture destinatarie.

Nelle more della completa diffusione del sistema di Protocollo Informatico all'intero Ateneo, l'Ufficio di Protocollo, utilizzando un'apposita funzione, visualizzerà solo i documenti i cui destinatari (tutti o parte) non sono provvisti di Protocollo Informatico e quindi provvederà a trasmettere il documento cartaceo alle strutture destinatarie sprovviste del sistema informatico. In tal caso, sarà sufficiente stampare una copia del documento (completo di timbro informatico) per ciascun destinatario.

Il componente applicativo appena descritto sarà in grado di selezionare, dalla lista di lavoro della struttura del Responsabile di sigla, tutti e soli i documenti interni (dotati di PG) che devono essere siglati ed assegnati. In questo modo, disponendo il Responsabile di sigla di uno strumento di selezione dei documenti da siglare, diviene superfluo l'utilizzo del documento cartaceo per l'avvio del processo di sigla.

Obiettivo 5 – Digitalizzazione dei procedimenti amministrativi rilevanti.

A partire dal 2007, si è avviato il processo di revisione e di dematerializzazione dei procedimenti amministrativi, mediante la gestione dell'iter dei procedimenti e l'istituzione di repertori specifici (quali, ad esempio: Decreti, Ordini di Servizio, Gare, Atti legali notificati, Omissis delibere, etc.). Di seguito, si riportano quelli più significativi ad oggi realizzati, oppure, avviati:

- La gestione del verbale digitale di Consiglio di Facoltà e di Dipartimento
- La convocazione degli Organi Collegiali
- L'autorizzazione e l'emanazione dei Decreti Rettorali, Direttoriali e Dirigenziali
- La comunicazione degli estratti delle delibere degli Organi Collegiali
- La registrazione degli atti legali e notificati
- L'iter di emissione dei bandi di gara
- La registrazione degli omissis delle delibere dei Consigli di dipartimento
- Gestione della interoperabilità di protocollo per la registrazione in entrata e in uscita di protocollo di messaggi PEC interoperabili: organizzazione servizio e addestramento incaricati

Obiettivo 6 – Avvio del sistema per la conservazione a norma dei documenti digitali contenuti nel sistema di Protocollo Informatico.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Di seguito, lo schema riepilogativo dei principali obiettivi perseguiti durante la fase di avvio e di esercizio del sistema:

Obiettivi	Azioni
Unificazione dei registri di protocollo delle strutture decentrate nel Protocollo Generale di Ateneo.	▪ Diffusione del Protocollo Informatico a tutte le strutture dell'Ateneo (UOR – Unità Organizzative Responsabili – di 1° livello).
Riduzione del flusso cartaceo (in ingresso) tra la Direzione Amministrativa e gli Uffici dell'Amministrazione Centrale assegnatari.	▪ Ampliamento delle funzionalità del Protocollo Informatico, in modo da consentire la gestione del workflow dell'iter documentale; ▪ Diffusione del Protocollo Informatico agli Uffici dell'Amministrazione Centrale; ▪ Organizzazione del processo di sigla presso la Direzione Amministrativa e le Ripartizioni.
Riduzione del flusso cartaceo tra le strutture dell'Ateneo.	▪ Eliminazione della minuta. Il documento originale, dopo la registrazione di protocollo, viene custodito dal mittente (solo flusso interno); ▪ Diffusione della firma digitale ai Responsabili delle strutture ed implementazione del timbro digitale.
Eliminazione del flusso cartaceo con enti esterni dotati di Protocollo Informatico a norma.	▪ Individuazione di soluzioni per la gestione della interoperabilità tra le caselle PEC dell'Ateneo, il Protocollo Informatico e gli enti esterni all'Ateneo.
Snellimento del carico di lavoro dell'Ufficio di Protocollo dell'Amministrazione Centrale.	▪ Realizzazione del processo informatico integrato di pre-registrazione di protocollo da parte degli Uffici dell'Amministrazione Centrale (limitatamente alla comunicazione di atti formali a strutture dell'Ateneo) e di sigla da parte del Responsabile.
Digitalizzazione dei procedimenti amministrativi rilevanti	▪ Istituzione di repertori specifici ▪ Utilizzo del PdP anche come strumento documentale di Workflow ▪ Avvio gestione della interoperabilità di protocollo per la registrazione in entrata e in uscita di protocollo di messaggi PEC interoperabili: organizzazione servizio e addestramento incaricati

Di seguito quindi, in modo coerente con quanto sopra riportato, viene illustrato il piano di massima degli interventi. Nella tabella, "Gruppo1", "Gruppo2" e "Gruppo3" individua l'insieme di strutture decentrate (Dipartimenti, Biblioteche e Centri

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

interdipartimentali di servizio e di ricerca) afferenti ai tre Poli (Polo delle Scienze e delle Tecnologie, Polo delle Scienze Umane e Sociali, Polo delle Scienze della Vita) che sono stati avviati in sequenza temporale nel corso del 2007:

PIANO DI DIFFUSIONE DEL PROTOCOLLO INFORMATICO E DELLA GESTIONE DEI FLUSSI DOCUMENTALI ELETTRONICI INTERNI ALL'ATENEO

	Amm.	Poli	CSI-DSF-DIS	Facoltà	Gruppo 1	Gruppo 2	Gruppo 3
> 2007							
15-11-2007			N/A	N/A	N/A	N/A	N/A
elettr 15-11-2007							
elettr 30-9-2007							
elettr 1-6-2007							
elettr 31-5-2007					N/A	N/A	N/A
carta 15-5-2007			N/A	N/A	N/A	N/A	N/A
carta 15-5-2007			N/A	N/A	N/A	N/A	N/A
carta 2-5-2007							
carta 15-4-2007			N/A	N/A	N/A	N/A	N/A
carta 15-4-2007			N/A	N/A	N/A	N/A	N/A
carta 1-1-2007							

Protocollo Informatico

Uffici: visualizzazione dei documenti assegnati. Il doc cartaceo, solo al I Assegnatario. Dopo , solo versione elettronica per i doc con Protocollo Generale.

DA, Direttori di Polo e Dirigenti Ripartizione: Sigla e smistamento dei documenti interni (già protocollati), cartacei, provenienti dalle altre UOR dotate di Protocollo Generale.

Tra UOR con Protocollo Generale, trasmissione di soli documenti elettronici (immagini scansionate dei documenti cartacei). Uscita: l'Ufficio consegna alla sigla solo minuta, poi inviata al proprio Uff. Protocollo e quindi restituita al mittente. Ingresso: i Responsabili di Sigla (UOR semplici) devono siglare ed assegnare elettronicamente i documenti ricevuti dalle altre UOR dotate di Protocollo Generale.

Solo per Amministrazione Centrale e Poli. Migliora ed integra e . Ingresso: Sigla elettronica dei documenti interni in ingresso da altre UOR con PG.
Uscita: Preregistrazione dei documenti interni da parte degli Uffici dell'Amministrazione Centrale e quindi sigla e registrazione. Stampa con Timbro digitale (Uff. Protocollo) ed invio, in fase transitoria, del doc cartaceo alle sole UOR sprovviste di Prot. Generale.

- Diffusione registrazione documenti sottoscritti con firma digitale
- Accreditamento in IPA della casella istituzionale PEC
- Diffusione registrazione messaggi PEC
- Repertori
- Interoperabilita' di protocollo
- Iter approvazione decreti
- Conservazione dei documenti informatici

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A8. MISURE DI SICUREZZA

A8.1. L'architettura tecnica del sistema

Di seguito, la scheda che riepiloga la piattaforma di riferimento del sistema eGrammata:

Scheda tecnica del sistema	
Modello architetturale applicativo	• **Integrazione applicativa: SOA** • **ESB: Spagic**
Gerarchia applicativa Multilivello	• **Presentation Logic : HTML- JSP – PHP –JavaScript** • **Application Logic: JServlet – Applet Java** • **Data Access: Stored procedure**
Piattaforma tecnologiche	• **DB Server**: **Linux Red Hat AS – Oracle 10g SE** • **S.O.: Linux Red Hat AS** • **Application Server**: **Tomcat** • **Web Server**: **Apache** • **HTTP browser: Explorer, Netscape, Mozzilla** • **Autenticazione LDAPs: OpenLDAP**

Piu' in dettaglio, la logica applicativa del prodotto E-Grammata per il **Protocollo Informatico** è ospitata su server di tecnologia Intel Xeon Pentium con S.O. Linux Red Hat AS Rel.4, Web Server Apache 2.054, Application Server Tomcat 5.0.28 e Cryptoserver JBOSS 4.0.

L'architettura del sistema è basata sull'integrazione applicativa dei seguenti componenti:

- HTML, JSP, PHP e JavaScript per la logica di presentazione;
- Jservlet, Applet Java e Stored Procedures per la logica applicativa;
- Stored Procedures per l'accesso ai dati;
- Protocollo SOAP (Service Oriented Architecture Protocol) per l'integrazione applicativa tra servizi sia in modalità "point-to-point" che tramite ESB (Enterprise Service Bus).

Dal punto di vista esecutivo, il servizio è erogato integrando i seguenti server:

- il WEB/ application server, per l'esecuzione della logica di presentazione e per la memorizzazione dei file contenenti le immagini dei documenti registrati (server tipo 05);

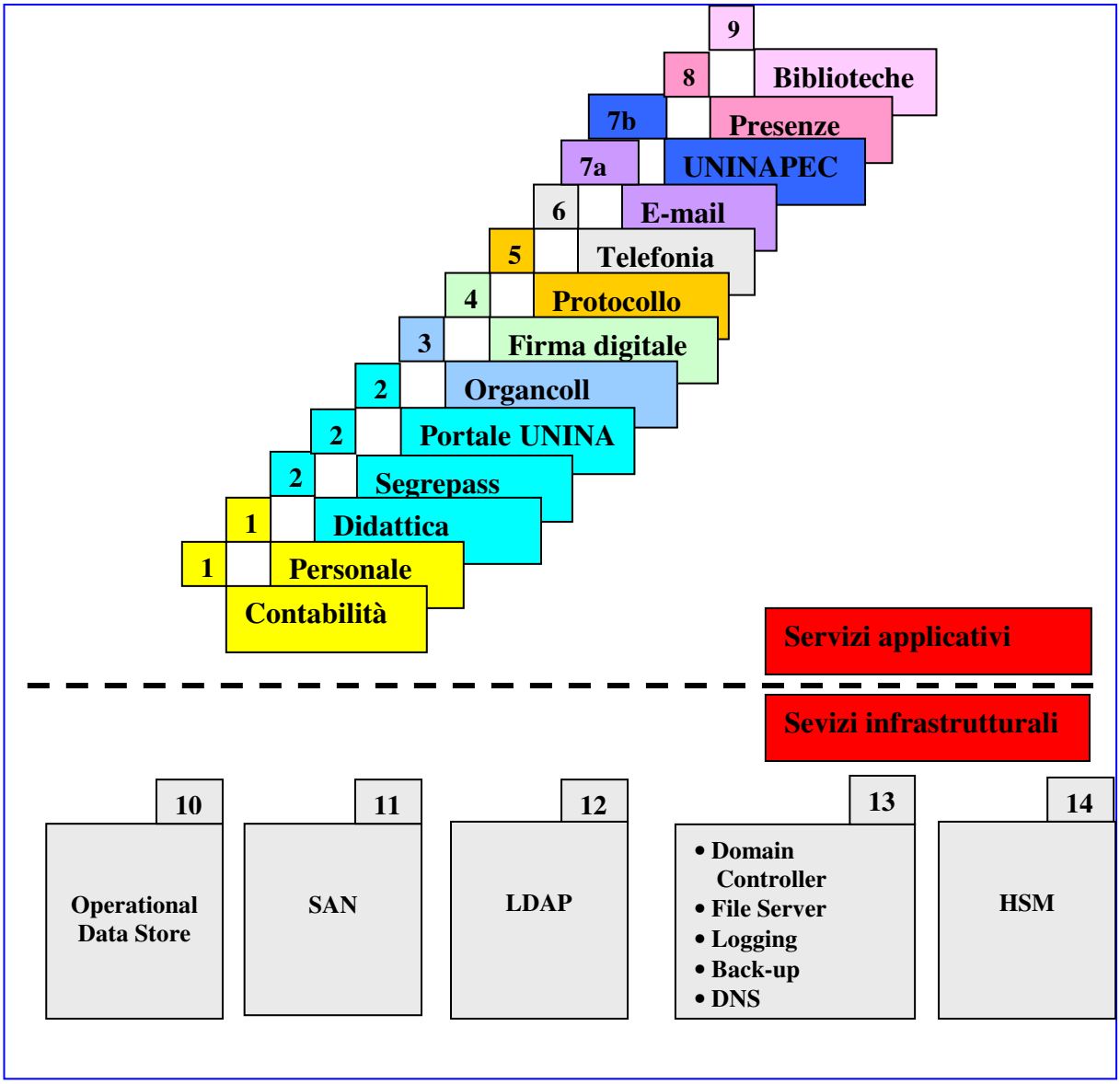
UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- l'Operational Data Store, basato su tecnologia Oracle 10g, risiedente su un server con 2 CPU, 4GB di memoria, 2 dischi Interni SCSI (mirrorati), 2 adattatori Ethernet 100mb e 2 adattatori Fibre Channel GB;
- SAN del CED del Centro Storico per la dislocazione fisica dei metadati relazionali di registrazione e per copia incrementale – eseguita in automatico con la frequenza di un minuto – delle immagini dei documenti protocollati e, dal 2008, le immagini dei documenti acquisiti mediante scanner;
- LDAP di Ateneo, per la autenticazione degli utenti.

A8.2. L'architettura applicativa

Nello schema seguente, si evidenzia come il servizio del PdP (server di tipologia 5) si avvalga di un insieme di servizi infrastrutturali, comuni a tutti i restanti servizi istituzionali di Ateneo, che risiedono nelle die server farm di Monte S. Angelo e del Centro Storico:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013



A8.3. L'Architettura di sicurezza

Le funzioni di sicurezza

Le funzioni di sicurezza che rappresentano gli obiettivi di sicurezza ICT rispetto ai quali misurare i sistemi implementati nell'ambito dell'Ateneo e, quindi, anche del sistema del PdP, recepiscono ed integrano le raccomandazioni contenute in "Generic headings" ITSEC ed nella Clausola 4 della norma BS 7799-1:2000.

Le funzioni di sicurezza previste sono:

Informatiche (INF)

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

1. Identificazione/Autenticazione
2. Controllo autorizzazione alle funzioni
3. Controllo autorizzazione ai dati
4. Tracciamento
5. Sistemi che evidenziano eventi anomali
6. Oscuramento dati di archivio
7. Sistemi riutilizzo supporti magnetici
8. Rilevazione e ripristino affidabilità sw
9. Qualità dei dati
10. Duplicazione dei dati/risorse
11. Controllo interscambio dati

Organizzative (ORG)

1. Norme di utilizzo
2. Procedure di gestione
3. Ruoli e responsabilità
4. Formazione
5. Sensibilizzazione e comunicazione

Logistiche (LOG)

1. Sistemi di rilevazione passiva
2. Sistemi di rilevazione attiva
3. Sistema di controllo accessi fisici
4. Sistemi di continuità di alimentazione
5. Infrastrutture

Le funzioni elencate sono in grado di garantire Integrità, Riservatezza e Disponibilità delle informazioni trattate nell'ambito del PdP, secondo la tabella di seguito riportata:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Classi di Funzioni di Sicurezza / Parametro di Sicurezza		I	R	D
INF	Identificazione/Autenticazione	X	X	
	Controllo autorizzazione alle funzioni	X	X	
	Controllo autorizzazione ai dati	X	X	
	Tracciamento	X	X	X
	Sistemi che evidenziano eventi anomali	X	X	X
	Oscuramento dati d'archivio		X	
	Sistemi riutilizzo supporti magnetici		X	
	Rilevazione e ripristino affidabilità sw	X		
	Qualità dei dati	X		
	Duplicazione dei dati/risorse			X
	Controllo interscambio dati	X	X	
ORG	Norme di utilizzo	X	X	X
	Procedure di gestione	X	X	X
	Ruoli e responsabilità	X	X	X
	Formazione	X	X	X
	Sensibilizzazione e comunicazione	X	X	X
LOG	Sistemi di rilevazione passiva			X
	Sistemi di rilevazione attiva			X
	Sistemi di controllo accessi fisici	X	X	X
	Sistemi di continuità di alimentazione	X		X
	Infrastrutture			X

Di seguito, dopo una breve sintesi dell'architettura di sicurezza del sistema del PdP, vengono illustrati nello specifico i meccanismi di sicurezza implementati per le funzioni di sicurezza precedentemente elencate.

A8.3.1.Descrizione generale dei meccanismi di sicurezza implementati nel PdP

L'abilitazione all'utilizzo di dati e funzioni del sistema di PdP è regolato da un sistema di profilatura degli utenti e di controllo delle loro credenziali integrato in E-Grammata.

La connessione al DB è effettuata mediante un utente di sistema, la cui password è esternamente configurabile e quindi periodicamente modificabile dall'Amministratore di Sistema DB. Anche la password dell'operatore immessa in fase di upload delle

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

immagini scansionate ed inviate al server di protocollo per la registrazione viene immessa in un campo oscurato ed è trasmessa in modo crittografato al server.

Inoltre, è stato implementato il meccanismo sicuro di accesso remoto al protocollo da internet. L'utente deve infatti prima autenticarsi al dominio "Amministrazione" immettendo le proprie credenziali di dominio (la cui password scade ogni tre mesi e deve essere modificata obbligatoriamente dall'interessato) e quindi quelle standard utilizzate per l'accesso alle applicazioni dell'area riservata dell'Università.

Tutte le modifiche a dati critici per l'intero funzionamento, secondo quanto prescritto dal DPR 445/2000, sono tracciate e visualizzabili a livello di interfaccia utente. I documenti protocollati (sia le immagini acquisite via scanner che i documenti informatici nativi) sono registrati in modo immodificabile, tramite associazione con l'impronta (hash) del documento stesso. Il sistema consente inoltre di tracciare e storicizzare anche le modifiche effettuate sugli allegati di una registrazione di protocollo e di registrare in modo immodificabile e, quindi, successivamente visualizzare le informazioni sull'autenticità ed integrità dei documenti sottoscritti con firma digitale.

Il sistema è inoltre controllato dal CED, mediante il software Nagios che consente di effettuare il monitoraggio dei sistemi e delle applicazioni istituzionali.

Esiste inoltre un meccanismo di time-out che chiude in automatico la sessione di lavoro se inattiva per un numero di minuti superiore a quello impostato dall'Amministratore (attualmente tale intervallo di tempo è stato impostato a 20 minuti).

Quotidianamente (dal lunedì al venerdì) è effettuato il back-up dei sistemi: due volte a settimana tale back-up è totale, nei restanti giorni è incrementale. Il sistema di I/O è configurato in modalità RAID 0+1. L'antivirus (Trend Micro) è aggiornato in modo automatico, non appena sono disponibili aggiornamenti. Anche l'aggiornamento del sistema per contrastare le vulnerabilità sul S.O. riscontrate è continuativo ed automatico. Non è automatico il sistema di aggiornamento dell'AS e dell'RDBMS, in quanto l'opportunità di effettuare l'aggiornamento, visto l'impatto che talvolta tali upgrade hanno sul funzionamento dell'intero sistema, va valutato di volta in volta (possibilmente implementato prima su di un ambiente di prova speculare rispetto a quello di esercizio).

Un sistema di configurazione software protegge inoltre i due server da connessioni indesiderate: sull'application server, sono inibite porte di comunicazione diverse da quella standard 80 dedicata al protocollo di comunicazione http e sono inoltre consentite solo le connessioni stabilite da client che risiedono sulla rete metropolitana dell'Ateneo (sono infatti disabilitate le connessioni da indirizzi internet o extranet). Per quanto riguarda l'ODS (Operational Data Store), accetta connessioni solo da risorse il cui IP address è contenuto in una limitata ACL (Access Control List).

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Al fine di garantire la massima disponibilità del servizio, a valle dell'espletamento di una procedura di gara, è stipulato un contratto di durata triennale per la fornitura del servizio di manutenzione ordinaria del sistema, con livelli di servizio ben definiti. Il Fornitore è nominato Responsabile del trattamento dei dati personali, anche se di prassi non accede ai dati personali contenuti nel DB del Protocollo Informatico, salvo i casi in cui deve effettuare problem determination. In tal caso, viene messa a disposizione del Fornitore una replica dei dati di esercizio (solo metadati) in ambiente di collaudo, in cui sono oscurati i dati personali (mittente e/o destinatari esterni, ed oggetto) delle registrazioni di protocollo.

A8.3.2.Le funzioni di sicurezza di tipo informatico

Sulla base di quanto detto, di seguito si riepiloga l'elenco delle funzioni di sicurezza di tipo informatico con la breve descrizione della funzione stessa e con la descrizione dei meccanismi di sicurezza messi in campo per ciascuna funzione:

- **Identificazione/Autenticazione**

Stabilisce e verifica in modo univoco l'identità dichiarata da un utente che vuole accedere al sistema. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni tra il sistema e l'utente. Si potranno avere altre interazioni solo dopo che l'operazione di identificazione e autenticazione è andata a buon fine. Le informazioni di autenticazione devono essere memorizzate in maniera che possano essere accedute solo da utenti autorizzati.

Coerentemente con quanto riportato nel documento Manuale_ad_uso_dei_responsabili_e_degli_incaricati, pubblicato sul portale dell'Ateneo all'indirizzo: http://www.unina.it/ateneo/attiNorme/sicurezza/index.jsp, i meccanismi previsti per l'identificazione/autenticazione al PdP sono basati sull'utilizzo di userid e password, con i seguenti livelli:

- password di accensione del PC (locale);
- userid e password per l'accesso alle risorse di rete (dominio);
- userid e password per l'accesso ai servizi.

Nel Manuale_ad_uso_dei_responsabili_e_degli_incaricati, sono impartite le seguenti direttive per una corretta gestione e custodia delle credenziali:

"La password di accensione è personale per cui l'Incaricato che utilizza l'elaboratore deve essere il solo a conoscerla e deve conseguentemente custodirla con cura affinché non venga accidentalmente diffusa.
Si sottolinea che l'attenta custodia della password di accensione va effettuata anche nell'interesse dello stesso utente al fine di non esporsi a dover rispondere di attività svolte da altri soggetti tramite il PC a lui assegnato.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Al fine di consentire l'uso del PC anche in caso di impedimento dell'Incaricato che lo utilizza normalmente, questi dovrà consegnare al Responsabile del trattamento dei dati della struttura una busta chiusa contenente la propria password e provvedere a sostituirla in occasione dell'adozione di una nuova password.

Il Responsabile del trattamento dei dati, in caso di impedimento temporaneo di un dipendente, qualora sia indispensabile utilizzare il PC a questi assegnato (anche per effettuare un intervento tecnico di manutenzione da parte del personale autorizzato), aprirà la busta contenente la relativa password e la fornirà ad altro dipendente per consentirgli l'utilizzo del detto PC. La busta, con l'indicazione della data della sua apertura, dovrà essere conservata a cura del Responsabile fino alla consegna della busta contenente la nuova password da parte del dipendente che è stato temporaneamente impedito."

Di seguito, si riportano le regole adottate per la gestione delle credenziali di autenticazione:

Regole per la gestione password di accensione del PC

È obbligatoria per i PC non collegati in rete, deve essere di lunghezza non inferiore a 8 caratteri o del massimo numero di caratteri consentiti dal sistema, deve essere modificabile dall'Incaricato e variata almeno ogni sei mesi. Nel caso in cui sul PC risiedano dati sensibili o giudiziari, tale password deve essere modificata a cura dell'incaricato almeno ogni tre mesi.

DESCRIZIONE	REGOLA
La password di S.O. può essere modificata dall'utente?	SI
Quale è la durata della password di BIOS?	6 mesi oppure 3 mesi nel caso di trattamenti con dati sensibili o giudiziari
La password viene revocata in caso di mancato utilizzo?	NO
La password ha una lunghezza minima?	SI, 8 caratteri, compatibilmente con i vincoli di lunghezza password consentiti dal S.O. del PC

Regole gestione credenziali per accesso alle risorse di rete

I PC dell'Amministrazione Centrale collegati alla rete d'Ateneo sono connessi ad un server di dominio che richiede obbligatoriamente, all'atto dell'accensione del PC, l'immissione delle credenziali per l'autenticazione al dominio di rete. Tali credenziali sono richieste, per ciascun Incaricato, dal rispettivo Responsabile UOR/UU mediante il modulo SICURDAT/B.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Coerentemente con quanto prescritto dal Disciplinare Tecnico allegato al D.Lgs. 196/2003, la password di dominio scade automaticamente ogni tre mesi e deve essere modificata dall'Incaricato. Qualora, scaduto tale termine, la password non è modificata per ulteriori sei mesi, le credenziali sono disattivate. L'istanza di riattivazione va presentata, a cura del Responsabile, mediante il modello SICURDAT/B. Infine, dopo cinque tentativi di connessione falliti, il codice identificativo (userid) è disabilitato. La richiesta di riabilitazione è effettuata dall'Incaricato mediante Contact Center del Centro Servizi Informatici d'Ateneo (CSI).

Inoltre, la userid per l'accesso al dominio è disabilitata a fronte di revoca esplicita dell'incarico da parte del Responsabile, oppure se non è utilizzata da almeno 6 mesi (Regola 7 dell'All. B del D. Lgs. 196/2003). Infine, le abilitazioni vanno confermata da parte del Responsabile della UOR/UU ogni anno, entro il 30 gennaio mediante compilazione dell'apposito modulo SICURDAT/B ed invio dello stesso alla Direzione Generale.

Tale userid è utilizzata dall'utente all'accensione del PC e consente la connessione della postazione al dominio di rete di appartenenza denominata "Amministrazione".

DESCRIZIONE	REGOLA
Lo USERID viene revocato in caso di mancato utilizzo?	SI, dopo sei mesi a partire dall'ultimo rinnovo di password non eseguito
Lo USERID viene disabilitato in caso di tentativi di connessione falliti?	SI, dopo al più 5 tentativi ripetutamente falliti di autenticazione
Quanti sono i tentativi di prova di una password di rete prima che lo USERID sia disabilitato?	5
La password di rete può essere modificata dall'utente?	SI
Quale è la durata della password di rete?	3 mesi
La password di rete ha una lunghezza minima?	SI, 8 caratteri

La password associata a ciascun userid abilitato deve essere di lunghezza almeno pari a otto caratteri. Gli utenti sono obbligati a modificarla almeno ogni 90 giorni.

Regole gestione credenziali per accesso ai servizi

Ad ogni utente delle applicazioni informatiche centralizzate è associata un'identità digitale con un codice identificativo personale (userid) ed un codice di reset password (puk) mediante il quale l'utente può creare o "resettare" la propria password. Ciascuna applicazione istituzionale, prima di effettuare la verifica del profilo di abilitazione dell'utente e, se abilitato, consentirgli l'accesso a dati e funzioni a cui questi è autorizzato, esegue il controllo di identità ed autorizzazione collegandosi all'LDAP del servizio centralizzato di autenticazione.

L'identità digitale viene assegnata (e cessata) dal C.S.I. all'utente in accordo con le politiche di Ateneo in materia di gestione delle identità digitali, contenute nel

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

"Regolamento di Ateneo in materia di utilizzo del servizio di posta elettronica @unina.it" o, nel caso per esempio di collaboratori esterni, non appena viene presentata la richiesta da parte del Responsabile UOR/UU, mediante comunicazione al Contact Center del C.S.I..

Lo userid è univoco e non condiviso con altri utilizzatori interni o esterni. Inoltre, è disabilitato a fronte di revoca esplicita dell'incarico da parte del Responsabile.

Le regole precedentemente esposte sono riepilogate nella tabella seguente:

DESCRIZIONE	REGOLA
Lo USERID per l'accesso ai servizi può essere modificata dall'utente?	NO, è assegnato da CSI
Quale è la durata dello USERID?	Dipende dal ruolo/funzione dell'utente e la sua durata [disciplinata dal Regolamento di Ateneo.
La password può essere modificata dall'utente?	SI
Quale è la durata della password?	Non scade
La password ha una lunghezza minima?	SI, 8 caratteri

Come già detto in precedenza, anche per il sistema del PdP, in fase di connessione da parte dell'utente al sistema, è il PdP che invoca il servizio di autenticazione centralizzato di Ateneo. In caso di controllo superato con successo, l'applicazione esegue il successivo controllo di autorizzazione alle funzionalità, come di seguito descritto.

- **Controllo autorizzazione alle funzionalità**

Garantisce che un utente possa espletare le sole operazioni di sua competenza, sulla base di profili generalizzati. Tra tali profili va previsto quello di amministrazione dei diritti di accesso e della loro verifica.

In dettaglio, con particolare riferimento a tale funzionale di sicurezza, il PdP consente la definizione e la gestione di utenti e di gruppi di utenti, con la specifica dei loro diritti di accesso ai dati, fino al massimo livello di granularità informativo presente. I profili di abilitazione previsti per gli utenti de PdP sono riportati nel modello SICURDAT/B disponibile all'indirizzo: http://www.unina.it/ateneo/attiNorme/sicurezza/index.jsp.

- **Controllo autorizzazione ai dati**

Garantisce che il processo e/o utente possano operare solo sui dati di propria competenza. Tra tali funzioni vanno previste quelle di amministrazione dei diritti di accesso e della loro verifica.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

In dettaglio, il sistema PdP consente la definizione e la gestione di utenti e di gruppi di utenti, con la specifica dei loro diritti di accesso ai dati, fino al massimo livello di granularità informativo presente, nonché di inibire completamente utenti o gruppi di utenti dall'accesso a determinati dati. Non è possibile, per chiunque non sia un utente autorizzato, di accordare o revocare diritti su di un dato. Allo stesso modo, solo gli utenti autorizzati (gli Amministratori di Sistema di tipo Applicazione) possono introdurre nuovi utenti o cancellare o sospendere utenti esistenti.

Il sistema che regolamenta le ACL (Access Control List) di accesso a documenti/fascicoli/metadati di registrazioni del PdP è basato principalmente, ma non in modo esclusivo, sull'afferenza della scrivania (o, postazione di lavoro) con cui l'utente si collega al sistema. Un utente può essere associato a una o più scrivanie, a seconda della posizione organizzativa e del profilo con cui deve operare in una data sessione di lavoro.

Per ogni tentativo di accesso ad un dato soggetto all'amministrazione di diritti, effettuato dagli utenti o dall'utente di un gruppo, il sistema verifica la validità delle richieste. Tentativi di accesso non autorizzato sono tracciati e respinti.

- **Tracciamento**

Registra gli accessi alle varie risorse del Sistema informatico rilevanti per gli aspetti di sicurezza. Non deve essere permesso agli utenti non autorizzati di accedere alle informazioni registrate. Deve essere inoltre possibile registrare selettivamente le azioni di uno o più utenti.

In dettaglio, il sistema PdP effettua il tracciamento delle operazioni che possono influenzare la sicurezza del sistema. Tali informazioni sono custodite nei log del sistema, accessibili esclusivamente agli Amministratori di Sistema..

Nella tabella seguente si riporta una lista degli eventi che sono tracciati.

Tipo evento
Uso del meccanismo di autenticazione e identificazione
Tentativi di esercitare diritti di accesso verso un oggetto di cui non si ha l'autorizzazione
Cancellazione di un oggetto
Scrittura o modifica di un oggetto
Lettura di un oggetto
Azioni da parte di utenti autorizzati che inficiano la sicurezza del sistema (inserimento o sospensione di utenti, mount di dischi, partenza e chiusura del sistema, ecc.)
Inserimento di dati da parte dell'utente
Definizione, assegnazione e revoca dei diritti di accesso a un oggetto

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Non deve essere concesso agli utenti non autorizzati di accedere ai dati di tracciamento.

I dati di tracciamento delle connessioni degli utenti via Web sono conservati per 6 mesi. A tale riguardo, è opportuno ricordare che per quanto attiene in modo specifico al Protocollo Informatico, al pari delle restanti applicazioni, l'Ateneo si limita a offrire tali servizi istituzionali a gruppi delimitati di utenze (dipendenti e studenti) solo a valle del controllo di autenticazione ed abilitazione dell'utente e non può essere considerato quale "fornitore di servizi di comunicazione elettronica accessibili al pubblico". Pertanto, le policy ed i meccanismi di sicurezza messi in campo dall'Ateneo sono compatibili con le previsioni del dlgs 196/2003, nonché - relativamente all'ambito delle connessioni a internet – alle "Linee guida del Garante per posta elettronica e internet". Con particolare riguardo alla conservazione dei log file contenenti i dati personali relativi agli accessi via web da internet o intranet di Ateneo (art. 6.2) , per conciliare il principio di pertinenza e non eccedenza, i log file sono periodicamente cancellati con il meccanismo di rotazione, in accordo con le previsioni dell'art.11 comma 1, lett. e) del Codice (sono cioè "conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati"), così come descritto già nel Documento Programmatico sulla Sicurezza 2011 approvato con Decreto Rettorale DR/2011/764 del 31.3.2011. Il periodo di retention per tali log file (log degli accessi) è stato successivamente ampliato da 15 gg. previsti nel suddetto DPS agli attuali 6 mesi, in modo tale da rendere conforme tale periodo con quello di conservazione dei file di log contenenti gli accessi degli Amministratori di Sistema, pari (in base alla normativa sugli AdS) a 6 mesi, come di seguito dettagliato.

Oltre ai log contenenti i dati di tracciamento delle connessioni utente, sono quindi registrati e sottoposti a conservazione i log, in cui sono presenti gli eventi associati all'accesso di Amministratori di Sistema. Tali log possono essere suddivisi in tre categorie:

- Log di Sistema;
- Log di Applicazione;
- Log di DB.

Per l'attuazione delle prescrizione del Garante della Privacy tutti i server da monitorare devono inviare i log ad una macchina remota per semplificarne l'amministrazione e il controllo e rendere vani i tentativi di un attacker di cancellare i log sulla macchina locale. I log devono essere inviati in maniera crittografata, poiché, avendo una struttura centralizzata, è necessario evitare che i log possano essere intercettati.

I log sul "log server" devono essere organizzati nelle tre categorie soprindicate.

Il software utilizzato per creare il secure remote log server è Syslog-NG.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Syslog-NG è uno strumento di tracciamento degli eventi di sistema prodotto da Balabit (www.balabit.com). Esso fornisce una gestione centralizzata dei log di tutte le device della rete sulla quale agisce, indipendentemente dalle piattaforme presenti. Inoltre fornisce diverse caratteristiche aggiuntive, inclusi filtri basati sul contenuto dei messaggi di log, gestione personalizzabile della memorizzazione delle informazioni raccolte e diverse capacità di analisi delle stesse. Uno dei principi di progettazione di Syslog-NG è quello di rendere il filtraggio dei messaggi molto più potente e sottile. Syslog-NG è capace di filtrare messaggi sulla base del loro contenuto, oltre che in base alla coppia opzione/priorità. In tal modo solo il messaggio che interessa veramente giungerà ad una specifica destinazione. Un altro principio di progettazione è stato quello di rendere più facile il trasferimento di log tra segmenti di rete protetti da firewall: il formato del nome dell'host permette di risalire facilmente alla macchina origine e alla catena di computer che ha trasportato il messaggio, anche se questo ha attraversato parecchi computer. L'ultimo principio è stato quello di scegliere un formato per il file di configurazione chiaro e potente. Per sicurezza, comunque, resta sempre una copia dei log sul server di origine.

Raccolti i log delle tre tipologie al "log server" viene applicata una politica di Backup del tipo GFS (Grandfather, Father, Son) settimanale con retention di 6 mesi con paradigma DDT (Disk, to Disk, to Tape). Infine, si provvede a calcolare l'hash del tar dei log per garantirne l'integrità.

I Log di Sistema

La conservazione dei log di sistema assicura l'archiviazione di tutti gli accessi alle macchine interessate da parte degli IT Administrator, nonchè le richieste di autenticazione (sia su dominio che su LDAP) e di autorizzazione ai server applicativi e la sincronizzazione della data e l'ora delle operazioni è assicurata da un server ntp a sua volta sincronizzato con l'istituto Galileo Ferraris di Torino.

I Log di Applicazione

Le applicazioni gestita dal CSI sono del tipo web. Il frontend è rappresentato o da un web server Apache o da un servlet container Tomcat. I log dei frontend hanno al proprio interno le informazioni necessarie per identificare gli accessi da parte degli Amministratori di Sistema, la sincronizzazione della data e l'ora delle operazioni è assicurata da un server ntp a sua volta sincronizzato con l'istituto Galileo Ferraris di Torino.

I Log di DB

I dbms gestiti dal CSI sono sia open source che proprietari (Mysql, Oracle…..). In entrambe le tipologie sono previsti log di connessione da client esterni. Quindi, attraverso i log di sistema vengono tracciate le connessione al db dalla consolle della macchina, attraverso i log di connessione al db sono tracciate le connessioni effettuate dai client (Toad, Sqlplus, …). Tutti i log hanno al proprio interno le informazioni necessarie per identificare gli accessi da parte degli Amministratori di Sistema, la

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

sincronizzazione della data e l'ora delle operazioni è assicurata da un server ntp a sua volta sincronizzato con l'istituto Galileo Ferraris di Torino.

- **Sistemi che evidenziano eventi anomali**

Permette di investigare sugli eventi che, discostandosi da determinate soglie, possono rappresentare una minaccia alla sicurezza. Devono essere presenti e documentati appositi strumenti per esaminare e gestire gli archivi registrati. Tali strumenti devono consentire di identificare selettivamente le azioni eseguite da uno o più utenti. Periodicamente controllano le registrazioni, per verificare casi anomali o sospetti. Permettono l'alert on-line o differito al superamento di opportune soglie di sicurezza predefinite.

Il sistema del PdP, al pari dei restanti sistemi infrastrutturali ed applicativi gestiti dal CSI è sottoposto a monitoraggio mediante il sistema Nagios in grado di inviare alert (anche preventivi) a console di sistema, mailing list e cellulari, al verificarsi di eventi anomali o al raggiungimento di prefissate soglie (ad es, di occupazione disco).

- **Oscuramento dati d'archivio**

Offre la possibilità di non permettere la lettura delle informazioni memorizzate nella base dati (per esempio tramite cifratura, compressione) garantendone la riservatezza.
In dettaglio, il sistema deve oscurare le informazioni ad alte sensibilità verso la riservatezza qualora queste vengano depositate su disco o altri supporti. L'obiettivo è di impedirne la lettura anche a chi può accedere ai supporti, ma non è autorizzato alla consultazione.

In particolare, il PdP permette di gestire registrazioni di tipo "riservato" che sono visualizzabili solo dagli utenti che dispongono di tale abilitazione specifica. Inoltre, il sistema consente di gestire i dati c.d. "sensibili": in tal caso, anche gli utenti potenzialmente abilitati ad accedere alla registrazione vedono i metadati oscurati e non possono visualizzare i documenti associati.

- **Sistemi di riutilizzo supporti magnetici**

Gestiscono il riutilizzo di risorse. Fra queste funzioni vi sono quelle di inizializzazione e cancellazione dei files contenenti informazioni di alta rilevanza rispetto alla riservatezza da supporti asportabili e riusabili, quali nastri magnetici, dischetti, DVD, hard disk o da supporti in output, come la cancellazione della schermata. Sui dischi è necessario proteggere le informazioni dei file eliminati dalla attività di disk scavenging (letteralmente significa raccolta di spazzatura) ovvero di lettura delle informazioni rimaste su disco relative a file cancellati. Per esempio, sui floppy disk vi è la possibilità di disk scavenging per cui, per un loro riutilizzo non basta eliminare i file, ma occorre rieseguire utilità di formattazione del tipo "zero filling".

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

In particolare, il sistema di PdP prevede che tutti i file temporanei o di spool utilizzati sono cancellati al termine del processo sia in caso di fine corretta o per errore, salvo esplicita configurazione del sistema tale da forzare, in condizioni particolari stabilite concordate dal CSI di concerto con il PdP, la conservazione di tali aree di appoggio, per una successiva loro cancellazione manuale da parte degli Amministratori di sistema. Tali scelte possono essere operate qualora si presentino situazioni di malfunzionamento del sistema tali da far propendere per la non cancellazione delle aree temporanee, al fine di minimizzare il rischio di perdita incontrollata dei dati. La configurazione del sistema viene quindi ripristinata a valle della risoluzione del problema.

- **Rilevazione e ripristino affidabilità software**

Permette l'analisi del software al fine di identificare, segnalare e correggere violazioni dell'integrità. Fra tali funzioni vi sono quelle di identificazione ed eliminazione dei virus, bombe logiche e "cavalli di troia", analisi del codice per verificare l'integrità degli eseguibili, la correttezza delle chiamate ai dati, ecc.

Il corretto deployment dell'applicazione del PdP è assicurata mediante un sistema di rilascio di patch incrementali che sono verificate in tre ambienti distinti (test, pre-produzione e collaudo) prima di essere installate in produzione. In particolare, gli unici soggetti abilitati ad eseguire tali operazioni in pre-produzione e produzione sono esclusivamente gli Amministratori di sistema SYS e DBA.

Il software di sistema sui server del PdP (application e DB) viene aggiornato manualmente, a fronte di ogni nuovo annuncio di vulnerabilità dei sistemi.

Inoltre, i server sono protetti da antivirus Trend Micro aggiornato automaticamente ogni ora. Anche i PC degli utenti sono protetti dall'attacco di virus, in quanto sono dotati di programma antivirus, centralizzato per i PC collegati in rete dell'Amministrazione Centrale, ed aggiornato automaticamente con cadenza giornaliera.

- **Duplicazione dati/risorse**

Garantisce la ridondanza delle risorse al fine di un loro ripristino in caso di malfunzionamenti, in modo da consentire il tempestivo ripristino del servizio. Tra tali funzioni vi sono quelle di salvataggio periodico (backup), mirroring dei dischi, logging.

Il salvataggio dei dati del PdP avviene con frequenza giornaliera. In particolare, per quanto riguarda i server su cui risiedono DB e sistema SAN, il back-up del sistema è eseguito quotidianamente in modalità incrementale dei dati su libreria centralizzata; il sabato viene eseguito inoltre il dump completo del sistema. Inoltre, viene eseguito ogni notte il back-up incrementale del DB del PdP e settimanalmente quello totale.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- **Controllo interscambio dati**

Assicura la sicurezza nelle trasmissioni di dati attraverso: autenticazione dell'originatore, integrità e riservatezza del contenuto del messaggio, non ripudio dell'originatore e del destinatario. Tale funzione di sicurezza può essere articolata conformemente allo standard X.509, nelle seguenti categorie di servizi di sicurezza:

- Autenticazione
- Controllo autorizzazioni
- Riservatezza dei dati
- Integrità dei dati
- Non ripudio

Di seguito se ne riporta una breve descrizione:

Autenticazione: garanzia che un'entità di pari livello in una comunicazione è quella che dichiara di essere;
Controllo autorizzazioni: impedimento dell'uso non autorizzato di una risorsa, includendo l'impedimento dell'uso di una risorsa in una maniera non autorizzata. In particolare, per ogni transazione via internet bisogna sempre utilizzare un sistema filtro di tipo "firewall";
Riservatezza dei dati: protezione dei dati da accessi non autorizzati, mediante sistemi di crittografia;
Integrità dei dati: la proprietà dei dati non deve essere alterata o distrutta: devono cioè essere riconosciute le manipolazioni non autorizzate di dati;
Non ripudio:

- Non ripudio di origine dei dati: il servizio garantisce al destinatario dei dati la prova della loro origine e protegge dal tentativo del mittente di negare falsamente la spedizione dei dati o il loro contenuto;
- Non ripudio del destinatario: il servizio garantisce al mittente dei dati l'avvenuta ricezione dei dati e protegge dal tentativo del destinatario di negare falsamente di aver ricevuto i dati o il loro contenuto.

Per quanto riguarda il PdP, attualmente viene garantito il controllo di autenticità dell'utente che si collega da internet mediante autenticazione aggiuntiva sul dominio "Amministrazione" mediante connessione su terminal server. Per quanto riguarda l'integrità dei dati immessi, il controllo è effettuato mediante calcolo dell'impronta (sha-1) di ciascun documento analogico e digitale. Il non ripudio dei documenti informatici è invece garantito mediante la firma digitale per la sottoscrizione degli atti scambiati all'interno della AOO e con altre AOO.

In aggiunta, per i documenti firmati digitalmente, il sistema PdP effettua il controllo di integrità e di autenticità prima della registrazione e blocca la registrazione nel caso in cui non sia superata la verifica di integrità del documento. Nel caso di controllo autenticità fallito (ad esempio, per certificato scaduto), l'operatore di protocollo può "forzare" la registrazione nel PdP, motivando l'operazione nel campo note della

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

registrazione. Nel caso di file firmati digitalmente, nel sistema PdP viene registrata l'intera busta crittografica in formato p7m e, quindi, anche l'impronta del documento firmato, in formato sha-256.

Infine, per quanto riguarda la trasmissione ed interscambio dei documenti informatici, il sistema di protocollo utilizza la PEC come mezzo trasmissivo per lo scambio di documenti amministrativi: in questo caso, l'infrastruttura certificata garantisce la provenienza del messaggio e, oltre alla data e ora certa, a fornirne certezza dell'integrità.

A8.3.3.Componente organizzativa della sicurezza

Di seguito, nel riepilogare e fornire una descrizione di ciascuna classe di sicurezza di tipo organizzativo, si fornisce la specifica relativa all'implementazione della classe stessa nell'ambito del servizio del protocollo informatico.

- **Norme di utilizzo:** documento rivolto agli utenti (Responsabili di UOR/UU ed Incaricati UOP) che descrive le norme comportamentali e procedurali da applicare per un utilizzo sicuro del Sistema. In particolare, sono state predisposti manuali, guide operative e presentazioni sul sito dell'egovernment all'indirizzo www.praxis.unina.it, nella sezione dedicata al protocollo informatico.
- **Procedure di gestione**: documento rivolto agli addetti alla gestione tecnica degli aspetti di sicurezza del Sistema che descrive le modalità di svolgimento delle attività di loro competenza. Tali procedure sono stabilite ed eseguite a cura del personale tecnico del C.S.I..
- **Ruoli e responsabilità**: descrizione di incaricati che gestiscono aspetti di sicurezza, con particolare riguardo alle responsabilità ed alle attività di loro competenza in ambito informatico.
  Per quanto riguarda i ruoli identificati sono i servizio di gestione del protocollo e dei flussi documentali, sono i seguenti:
  - Responsabile UOR/UU, coincidente con la figura del responsabile del trattamento dei dati personali, formalmente nominato dal Rettore o dal Direttore Generale;
  - Incaricato del trattamento dei dati personali. Il dipendente o fornitore esterno individuato per operare nell'ambito del sistema, secondo un profilo di abilitazione definito dal responsabile formalizzato tramite compilazione di appositi modelli (SICURDAT/B) sottoposti all'autorizzazione del Direttore Generale e quindi inoltrati al C.S.I. per gli aspetti legati alla configurazione del sistema di abilitazione. I profili di sicurezza previsti sono stati precedentemente riportati;
  - Amministratori di sistema. Per quanto attiene al personale interno o esterno a cui è conferito il compito di sovrintendere alle risorse del sistema

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione, l'Università ha individuato i seguenti profili:

- AdS-Sistema
- AdS-Database
- AdS-Rete
- AdS-Applicazione

Gli Amministratori di Sistema (AdS), dipendenti o non dell'Ateneo, designati in virtù del Provvedimento a carattere generale del Garante per la Protezione dei Dati Personali del 27.11.2008 titolato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", devono garantire, sulla base del proprio profilo di AdS, il rispetto delle misure minime di sicurezza di seguito elencate. Per quanto riguarda le unità di personale interne, tali figure sono tutti incaricati afferenti al C.S.I. e sono, pertanto nominati dal Presidente del C.S.I. che provvede quindi ad inviare ogni anno al Direttore Generale l'elenco aggiornato degli AdS, unitamente al curriculum vitae di ciascuno di loro. Di seguito, i compiti svolti da ciascuna figura di AdS.

Profilo AdS-Sistema

- assicurare la gestione ed il corretto funzionamento dei sistemi di autenticazione ed autorizzazione degli utenti sui sistemi server in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sui sistemi server in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso:
- predisporre e rendere funzionanti le copie di sicurezza (backup e recovery) dei sistemi server in uso;
- predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi server in uso. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- predisporre sugli elaboratori del sistema informativo i meccanismi per la protezione dei sistemi contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale, mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale;
- adottare di ulteriori misure di sicurezza previste dal Codice per i trattamenti di dati sensibili o giudiziari, finalizzate alla protezione dei dati contro l'accesso abusivo, alla custodia o alla distruzione dei supporti rimovibili su cui sono memorizzati i dati, al ripristino dell'accesso ai dati in caso di

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

Profilo AdS-Database

- assicurare la gestione ed il corretto funzionamento dei sistemi di autenticazione ed autorizzazione degli utenti sui database in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sui database in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso:
- predisporre e rendere funzionanti le copie di sicurezza (backup e recovery) dei database in uso;
- predisporre sistemi idonei alla registrazione degli accessi logici ai database in uso. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale;
- adottare ulteriori misure di sicurezza previste dal Codice per i trattamenti di dati sensibili o giudiziari, finalizzate alla protezione dei dati contro l'accesso abusivo, alla custodia o alla distruzione dei supporti rimovibili su cui sono memorizzati i dati, al ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

Profilo AdS-Rete

- assicurare la gestione ed il corretto funzionamento degli apparati di rete;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati ad accedere a tali apparati, in qualità di amministratori, provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso:
- predisporre e rendere funzionanti soluzioni per aumentare la disponibilità della rete;
- predisporre sugli apparati di rete meccanismi per la protezione dei sistemi contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale, mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
- predisporre ed aggiornare i programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale;
- adottare di ulteriori misure di sicurezza previste dal Codice per i trattamenti di dati sensibili o giudiziari, finalizzate alla protezione dei dati contro l'accesso abusivo, alla custodia o alla distruzione dei supporti rimovibili su cui sono memorizzati i dati, al ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi compatibili con i diritti degli interessati e non superiori a sette giorni.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Profilo AdS-Applicazione

- assicurare la gestione ed il corretto funzionamento delle applicazioni e dei sistemi di profilatura degli utenti sulle applicazioni in uso;
- eseguire la verifica periodica, ogni 6 mesi, degli utenti autorizzati sulle applicazioni in uso provvedendo alla cancellazione degli utenti non più in possesso dell'autorizzazione all'accesso;
- predisporre ed aggiornare i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, con cadenza almeno semestrale.

- **Formazione**: attività tesa a istruire gli addetti e gli utenti che operano su risorse sensibili al fine di utilizzare al meglio i dispositivi di sicurezza progettati. Relativamente a tale aspetto, l'Amministrazione ha organizzato corsi di addestramento degli incaricati, secondo il piano descritto nell'allegato 6 del presente MdG.

- **Sensibilizzazione e comunicazione**: attività svolta verso tutti gli utenti per sensibilizzarli alle problematiche generali legate alla corretta gestione dei flussi documentali e del trattamento dei documenti digitali.

  L'attività consiste nella divulgazione:

  - Della normativa di riferimento,
  - Delle regole e delle prassi definite nell'ambito dell'Amministrazione,
  - Dei ruoli e delle responsabilità di ciascuno nell'ambito del processo di gestione a norma dei documenti amministrativi dell'Ateneo.

  L'obiettivo è di creare con interventi sistematici una maggiore coscienza e considerazione alle problematiche legate ad una corretta attuazione delle norme e dei regolamenti interni per una corretta gestione dei flussi documentali e del protocollo.

  L'attività si è fino ad oggi esplicata con specifici interventi mediante l'organizzazione di seminari, riunioni, corsi e circolari.

A8.3.4.Componente infrastrutturale della sicurezza

Con particolare riguardo ai locali che ospitano i server utilizzati per il servizio Protocollo Informatico, di seguito si riportano le funzioni di sicurezza previste:

- Sistemi di rilevazione passiva: impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo senza attivare contromisure.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- Sistemi di rilevazione attiva: impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo e attivando una specifica contromisura (impianti fissi di soppressione incendio).

- Sistemi di controllo accessi fisici: impianti che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati (ad esempio, porta di accesso unica con chiave, sistema di allarme per le uscite di emergenza).

- Sistemi di continuità di alimentazione: impianti che garantiscono una continuità dell'alimentazione elettrica ai sistemi, almeno per una chiusura ordinata.

- Infrastrutture: accorgimenti generici sugli edifici e disposizione dei locali al fine di garantire la sicurezza (edifici antisismici, uscite di sicurezza allarmate, separazione ambienti a rischio, condizionamento ambiente, estintori, armadi ignifughi,ecc.).

Di seguito, la tabella che riepiloga i dispositivi di sicurezza di tipo logistico previsti ad oggi nei locali del CED CSI, del Centro Storico e di Monte S. Angelo, in cui sono ubicati i dispositivi (server, sistema autenticazione, back-up, rete, etc.) su cui insiste il sistema di PdP:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Dispositivo	CED CSI (Centro Storico)	CED CSI (MSA)
Porta di accesso unica con chiave/ badge/ biometrico (Sistemi di controllo accessi fisici)	✓	✓
Impianto antintrusione (Sistemi di controllo accessi fisici)	✓	✓
Videosorveglianza (Sistemi di controllo accessi fisici)	✓	✓
Rilevatore incendio (Sistemi di rilevazione passiva)	✓	✓
Rilevatore di fumo (Sistemi di rilevazione passiva)	✓	✓
Impianti fissi soppressione incendio (Sistemi di rilevazione attiva)	✓	
Estintori (Infrastrutture)	✓	✓
Armadi ignifughi e stagni (Infrastrutture)	✓	✓
Condizionamento ambiente e segnalazione anomalie (Infrastrutture)	✓	✓
Quadro elettrico chiuso a chiave (Infrastrutture)	✓	✓
Sistema UPS (Sistemi di continuità di alimentazione)	✓	✓
Inverter per stabilizzazione (Sistemi di continuità di alimentazione)	✓	✓
Gruppo elettrogeno (Sistemi di continuità di alimentazione)	✓	✓

A8.3.5.Le minacce e gli agenti

Le minacce che prese in considerazione dal Piano della Sicurezza per il PdP appartengono alle seguenti tipologie:

1. Furti
2. Frodi o malversazioni (computer crime)
3. Danneggiamento
4. Manipolazioni di dati e/o programmi
5. Perdita di privacy
6. Errori sui dati e programmi
7. Utilizzo di software illecito
8. Divulgazione di dati e programmi
9. Utilizzo illegale di risorse
10. Indisponibilità dei sistemi
11. Inagibilità dei locali

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Con il termine *Agente* si intende la materializzazione di una minaccia in funzione del tipo di portatore possibile. Gli agenti sono classificabili come segue:

- **A - Agenti non umani**

A1. Eventi Naturali

1. Alluvione
2. Terremoti
3. Allagamenti
4. Trombe d'aria
5. Fulmini
6. Meteoriti
7. Altri eventi meteorologici

A2. Eventi Accidentali

1. Fuoco agli impianti
2. Fuoco ai locali
3. Allagamento
4. Interruzione energia elettrica
5. Interruzioni alla rete
6. Avarie dei servizi ausiliari
7. Indisponibilità dei sistemi
8. Trasporti dei beni informatici
9. Altri incidenti

- **B - Agenti umani**

B1. Persone identificate - cioè quelle persone delle quali l'Azienda possiede, o può recuperare, i dati personali, in quanto sono legittimate all'ingresso presso le proprie sedi.

B2. Persone ignote.

A8.3.6.La tabella di correlazione minacce/funzioni di sicurezza

Di seguito, la tabella dove si indica quali minacce vengono contrastate da ciascuna funzione di sicurezza:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Codice Minaccia / Classi di Funzioni di Sicurezza	T01 FURTI	T02 FRODI	T03 DANNEGGIAMENTO	T04 MANIPOL dati e/o prog	T05 PERDITAPRIVACY	T06 ERRORI SU dati e/o prog	T07 UTIL. SW ILLECITO	T08 DIVULGAZIONE dati e/o prog	T09 UTIL. ILLEGALE ris	T10 INDISPONIBILITÀ sist	T11 INAGIBIL. LOCALI
Funzioni HW/SW											
Identificazione/Autenticazione	X	X		X	X		X	X	X		
Controllo autorizzazione alle funzioni		X		X	X	X	X	X	X	X	
Controllo autorizzazione ai dati	X	X		X	X	X	X	X	X		
Tracciamento	X	X	X	X	X	X	X	X	X	X	
Sistemi che evidenziano eventi anomali	X	X	X	X	X	X	X	X	X	X	
Oscuramento dati d'archivio					X			X			
Sistemi riutilizzo supporti magnetici					X			X			
Rilevazione e ripristino affidabilità sw			X	X		X					
Qualità sw/dati			X	X		X					
Duplicazione dei dati / risorse	X		X	X		X				X	X
Controllo interscambio dati		X		X	X	X		X	X		
Funzioni organizzative											
Norme di utilizzo	X	X	X	X	X	X	X	X	X	X	
Procedure di gestione	X	X	X	X	X	X	X	X	X	X	
Ruoli e responsabilità	X	X	X	X	X	X	X	X	X	X	
Formazione	X	X	X	X	X	X	X	X	X	X	
Sensibilizzazione e comunicazione	X	X	X	X	X	X	X	X	X	X	
Funzioni Logistiche											
Sistemi di rilevazione passiva	X		X							X	X
Sistemi di rilevazione attiva	X		X							X	X
Sistemi di controllo accessi fisici	X		X		X			X	X	X	
Sistemi di continuità di alimentazione			X							X	
Infrastrutture			X								X

Utilizzando tale matrice, in base alle misure di sicurezza adottate, è quindi possibile determinare il grado di copertura del sistema PdP rispetto alle minacce considerate.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A8.3.7.Determinazione del grado di copertura e del rischio residuo

Sulla base delle funzioni di sicurezza specificate, della distribuzione in architettura dei dati trattati e dei meccanismi di sicurezza implementati per gestire il sistema del Protocollo Informatico, si può quindi procedere all'analisi qualitativa del grado di copertura e quindi alla determinazione del rischio residuo.

Più in dettaglio, utilizzando le informazioni precedentemente riportate, è possibile compilare la seguente griglia, dove si indica la copertura per ciascuna funzione per classe e parametro di sicurezza: un pallino bianco significa che non sono implementati meccanismi di sicurezza; uno nero significa che la funzione è realizzata in modo adeguato rispetto ai requisiti minimi normativi richiesti per un sistema di protocollo "a norma" e coerente con le policy di sicurezza dell'Ateneo descritte in precedenza. Il simbolo "⊙", infine, indica che la funzione di sicurezza non è implementata in modo completo, rispetto alle specifiche precedentemente fornite e va quindi adeguata, ovvero migliorata.

Nel computo del punteggio totale per ciascuna classe/parametro di sicurezza, l'attribuzione dei punti è la seguente alle voci caratterizzate dal simbolo "●", 1 punto, a quelle caratterizzate dal simbolo "⊙", 0,5 punti. Il punteggio totale è dato dalla sommatoria di tali valori.

Infine, il grado di copertura, espresso come Basso, Medio e Alto, viene determinato calcolando secondo la tabella di seguito riportata:

Percentuale	GRADO COPERTURA
0 - 33 %	Basso (B)
34 – 74 %	Medio (M)
75 – 100 %	Alto (A)

Di seguito si riporta quindi la tabella valorizzata per il sistema del Protocollo Informatico:

SISTEMA PROTOCOLLO INFORMATICO						
Classe di Rilevanza	ALTA			MEDIA		
Parametro di sicurezza / Classi di Funzioni di sicurezza	I	R	D	I	R	D
Identificazione/Autenticazione	⊙	⊙		⊙	⊙	
Controllo autorizzazione alle funzioni	●	●		●	●	
Controllo autorizzazione ai dati	⊙	⊙		⊙	⊙	
Tracciamento	●	●	●	●	●	●
Sistemi che evidenziano eventi anomali	●	●	●	●	●	●

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

SISTEMA PROTOCOLLO INFORMATICO						
Classe di Rilevanza	**ALTA**			**MEDIA**		
Parametro di sicurezza / **Classi di Funzioni di sicurezza**	**I**	**R**	**D**	**I**	**R**	**D**
Oscuramento dati d'archivio		●				
Sistemi riutilizzo supporti magnetici		⊙				
Rilevazione e ripristino affidabilità software	⊙			⊙		
Qualità dei dati	●			●		
Duplicazione dei dati/risorse			⊙			⊙
Controllo interscambio dati	⊙	⊙		⊙	⊙	
Norme di utilizzo	●	●	●	●	●	●
Procedure di gestione	●	●	●	●	●	●
Ruoli e responsabilità	⊙	⊙	⊙	⊙	⊙	⊙
Formazione	⊙	⊙	⊙			
Sensibilizzazione e comunicazione	⊙	⊙	⊙	⊙	⊙	⊙
Sistemi di rilevazione passiva			●			●
Sistemi di rilevazione attiva			●			●
Sistemi di controllo accessi fisici	●	●	●	●	●	●
Sistemi di continuità di alimentazione	●		●	●		●
Infrastrutture			●			●
Totale	**11,5**	**10,5**	**11**	**11**	**8,5**	**10,5**
Punteggio massimo	**15**	**14**	**13**	**14**	**11**	**12**
Percentuale	**77**	**75**	**85**	**78**	**77**	**87**
GRADO DI COPERTURA	**A**	**A**	**A**	**A**	**A**	**A**

Da quanto detto risulta che il sistema, di recente progettazione ed implementazione, presenta un grado di copertura accettabile rispetto al rischio di perdita o di danneggiamento dei dati. Sono comunque da irrobustire, con particolare riguardo alla tutela della riservatezza, le seguenti funzioni:

1) la fase di autenticazione, mediante l'introduzione del meccanismo di disabilitazione della userid se non utilizzata per lasso di tempo superiore ai sei mesi. Tale meccanismo, insieme a quello della disabilitazione della userid a fronte di cinque tentativi di connessione falliti ed a quello della modifica obbligatoria della password ogni tre mesi, potrebbe essere implementato, in maniera centralizzata, sul server LDAP.
2) la duplicazione dati e risorse, mediante la messa in esercizio di una architettura Oracle RAC, l'avvio del sistema di conservazione e la definizione di uno strutturato BCP;
3) l'interscambio dati, mediante l'utilizzo del protocollo https in fase di autenticazione degli utenti al servizio e di connessione dei processi all'Operational Data Store del PdP.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A9. CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO

Di seguito, si riportano alcune disposizioni impartite dal Direttore Generale ai responsabili UOR/UU/RPA dell'Amministrazione Centrale per la consegna, il prelievo e la consultazione della documentazione custodita nell'archivio corrente del palazzo degli Uffici.

L'archivio corrente del palazzo degli Uffici

I locali appositamente destinati all'archivio in argomento devono essere presidiati da una unità di personale afferente all'ufficio Archivio con mansioni di custodia e controllo sul prelievo e ricollocazione della documentazione di volta in volta occorrente agli uffici medesimi.

Il personale addetto al controllo dovrà consentire l'accesso all'archivio esclusivamente al personale munito di autorizzazione firmata dal capo dell'ufficio o del reparto ed opportunamente esibita.

I responsabili di struttura organizzano, pertanto, il servizio di prelievo, smistamento e ricollocazione della documentazione individuando, con le modalità sopra indicate, un proprio addetto che, durante l'orario di apertura al pubblico o al ricorrere delle eventuali esigenze lavorative della struttura, dovrà recarsi presso i locali adibiti ad archivio.

Gli archivi di deposito (Sede Centrale, Botteghelle, Monte Sant'Angelo, Agnano)

Di seguito, si riportano alcune disposizioni impartite dal Responsabile Archivi ai responsabili UOR/UU/RPA per la consegna, il prelievo e la consultazione della documentazione gestita dal servizio Archivio.

a) L'archiviazione. La restituzione di documenti in consultazione.

I documenti da archiviare devono essere consegnati all'Incaricato dell'Ufficio Archivio, previo informale preavviso, ogni giovedì dalle ore 9.00 alle ore 13.00 ed in caso di festività il successivo giorno lavorativo.

Dovranno essere accompagnati dalla relativa nota di trasmissione, utilizzando apposito modello, con l'indicazione dettagliata della documentazione da archiviare.

Analogo iter dovrà essere seguito per la restituzione di documentazione o fascicoli già archiviati e temporaneamente in consultazione.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

Qualora la richiesta di archiviazione concerna un numero considerevole di fascicoli pacchi e contenitori, la trasmissione dovrà essere preventivamente concordata con il capo dell'Ufficio Archivio e con il responsabile dei Servizi Generali. Il detto responsabile disporrà, d'intesa con il capo dell'Ufficio Archivio il trasporto della documentazione in argomento dall'Ufficio interessato ai locali di archivio cui la stessa è destinata.
Alla consegna della documentazione all'Ufficio Archivio dovrà presenziare un Incaricato dell'ufficio richiedente.

b) La consultazione di documenti archiviati.

La consultazione di documenti archiviati comporta normalmente l'accesso a dati personali. Pertanto si ritiene utile riportare in questa sede le disposizioni relative all'archiviazione di documenti e fascicoli.

b.1) La consultazione presso l'archivio della Sede Centrale:

Le richieste di consultazione di documenti e fascicoli archiviati nell'archivio della Sede Centrale devono essere inoltrate all'Ufficio Archivio, a mezzo degli appositi modelli per la consultazione di documentazione non relativa agli studenti e per la consultazione di fascicoli degli studenti.

L'ufficio provvederà ad evadere, ove possibile, in tempo reale e in stretto ordine cronologico tutte le richieste avanzate dagli utenti ogni giovedì dalle ore 9.00 alle ore 13.00 ed, in caso di festività il successivo giorno lavorativo.

Gli stessi uffici, nel giorno e nelle ore sopra indicate, avanzeranno le opportune richieste, ritirando contemporaneamente, laddove possibile, la relativa documentazione.

Nel mese di agosto l'Ufficio Archivio assicurerà il servizio nello stesso giorno e con le stesse modalità, previa richiesta telefonica da parte degli uffici interessati.

L'urgenza della richiesta, debitamente motivata, sarà valutata dal Dirigente della Ripartizione. Le chiavi di accesso ai locali dell'archivio devono essere consegnate dai custodi della sede centrale unicamente al personale dell'ufficio archivio che sarà opportunamente indicato dal Capo Ufficio.

b.2) La consultazione presso gli archivi di via Botteghelle e di Monte Sant'Angelo

Le richieste relative a documentazione e fascicoli conservati negli archivi di via Botteghelle e di Monte Sant'Angelo devono essere inoltrate attraverso i modelli illustrati in precedenza.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

L'evasione delle richieste avverrà in stretto ordine cronologico, fatte salve le motivazioni di urgenza opportunamente indicate dal richiedente e valutate dal Capo Ufficio Archivio.

L'Ufficio Archivio provvederà a trasmettere i fascicoli e la documentazione richiesti con un apposito elenco riportante la indicazione dell'ufficio richiedente.
Il responsabile dei Servizi Generali disporrà affinché siano prelevati i fascicoli e la documentazione per la relativa consegna e provvederà, altresì, a restituire all'Ufficio Archivio copia dell'elenco di trasmissione di cui sopra, completo delle firme di ricevuta.

Eventuali autorizzazioni di accesso ai locali adibiti ad archivio in deroga alle presenti disposizioni saranno concesse, di volta in volta, per iscritto, dal capo dell'Ufficio Archivio, che provvederà a conservare copia della richiesta e della autorizzazione.

I fascicoli consultati devono essere utilizzati secondo le modalità dettate per i documenti contenuti negli archivi correnti.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A10. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Oltre alle tipologie documentarie escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000, sono altresì escluse quelle elencate di seguito:

A10.1. Documenti in arrivo

- Documentazione in arrivo già soggetta, direttamente o indirettamente, a repertoriazione (es. fatture, vaglia, assegni)
- biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- avvisi di pagamento – comunicazioni di bonifici bancari
- avviso di vacanza posti personale tecnico-amministrativo presso altri atenei (art. 46 CCNL), pubblicati all'albo
- bandi di altri atenei di selezione per assegni per la collaborazione ad attività di ricerca
- certificati medici, con e senza lettera di trasmissione
- comunicati stampa ministeriali, CRUI, ecc., salvo espressa richiesta di protocollazione da parte della UOR
- comunicazione da parte di enti di bandi di concorso
- comunicazione trasferimento sede legale
- comunicazioni cambio banca di fornitori
- convocazioni dei CCL e dei Consigli di Diparimentoche pervengono per conoscenza all'amministrazione centrale
- estratti conto bancari
- giustificativi di assenza del personale
- lettere accompagnatorie di fatture
- missioni del personale
- mod. 730: corrispondenza di spedizione all'Ateneo e modelli
- offerte/preventivi di terzi non richiesti o non inerenti a gare
- progetti formativi e di orientamento – stage
- registri lezioni
- restituzioni dei buoni mensa da parte dei ristoratori o ditte convenzionate
- richiesta conferma di autocertificazione
- richiesta di rimborso spese e missioni di commissari interni ed esterni
- richiesta rilascio certificati di servizio personale docente di ruolo e non di ruolo
- richiesta rilascio certificati di servizio personale tecnico amministrativo
- richiesta rilascio certificazioni studenti
- richieste di ferie
- richieste di permesso orario del personale tecnico amministrativo

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- rimborsi piccole spese

A10.2. Documenti in partenza

- Documentazione in partenza già soggetta, direttamente o indirettamente, a repertoriazione (es. fatture, vaglia, assegni)
- assegnazione buoni mensa ai dipendenti
- cedolini stipendio
- certificati di servizio personale docente di ruolo e non di ruolo
- certificati di servizio personale tecnico amministrativo (a tempo determinato o indeterminato, CEL)
- certificati situazioni retributive e contributive personale strutturato e non strutturato
- certificazioni non meccanizzate
- certificazioni studenti (tipologie)
- modello CUD
- report delle presenze

A10.3. Documenti interni

- richieste del servizio di pulizie
- richieste di facchinaggio
- richieste di fornitura di cancelleria
- richieste di piccole manutenzioni
- richieste di sopralluoghi ai servizi tecnici
- richieste di sopralluoghi archivistici

A10.4. Eccezioni

Sono tipologie documentali espressamente da protocollare le seguenti:

- fatture in "ritardo" pena interessi di mora
- tutti i documenti di norma non soggetti a protocollazione per ragioni archivistiche e organizzative ricevuti in ritardo che la UOR ritiene di inviare al Servizio Archivio e Protocollo per la registrazione
- comunicati stampa dell'Amministrazione

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A11. ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati. Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

Di seguito, l'elenco dei documenti soggetti a registrazione nel protocollo particolare:

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- Corrispondenza legata a vicende di persone o a fatti privati o particolari;
- Le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241; dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A12. TITOLARIO DI CLASSIFICAZIONE

TITOLO	CLASSE		DESCRIZIONE
I			**Amministrazione**
I	1		Leggi e rispettive circolari applicative
I	2		Statuto
I	3		Regolamenti
I	4		Protezione dei dati personali
I	5		Stemma, gonfalone e sigillo
I	6		Sistema informativo e sistema informatico e telematico
I	7		Archivio e protocollo
I	8		Informazioni e relazioni con il pubblico
I	9		Strategie per il personale, organigramma e funzionigramma
I	10		Rapporti sindacali e contrattazione decentrata
I	11		Controllo di gestione
I	12		Statistica e auditing
I	13		Elezioni
I	14		Attività culturali, sportive e ricreative
I	15		Editoria ed attività informativo-promozionale interna ed esterna
I	16		Onorificenze, cerimoniale ed attività di rappresentanza
I	17		Interventi di carattere politico, economico, socio-culturale e umanitario
I	18		Nomine in enti ed organi esterni
I	19		Politiche e interventi per le pari opportunità
I	20		Sistema qualità
I	21		Adempimenti in materia di prevenzione e repressione della corruzione
II			**Organi di Governo, gestione, controllo, consulenza e garanzia**
II	1		Rettore con relative commissioni e comitati, anche misti
II	2		Prorettore e delegati del Rettore
II	3		Senato accademico con relative commissioni e comitati
II	4		Commissione etica di Ateneo
II	5		Consiglio di Amministrazione con relative commissioni e comitati
II	6		Direttore Amministrativo
II	7		Presidente e Direttore del Polo
II	8		Consiglio di Polo con relative commissioni
II	9		Consulta di Polo
II	10		Consiglio degli studenti
II	11		Conferenza dei Rettori delle Università Italiane
II	12		Collegio dei revisori dei conti
II	13		Nucleo di valutazione
II	14		Comitato per lo sport universitario
II	15		Comitato per le pari opportunità
II	16		Collegio dei garanti
II	17		Difensore Civico di Ateneo
II	18		Collegio arbitrale di disciplina
II	19		Preside di Facoltà
II	20		Consiglio di Facoltà con relative commissioni
II	21		Giunta di Facoltà
II	22		Presidente e Consiglio del Corso di studio, di Classe o di Coordinamento tra Corsi di studio

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

TITOLO	CLASSE		DESCRIZIONE
II	23		Direttore e Consiglio della scuola di specializzazione
II	24		Consiglio degli studenti di Facoltà
II	25		Direttore e Consiglio del Dipartimento o del Centro di ricerca o di servizio
II	26		Giunta del Dipartimento
II	27		Comitato scientifico e Direttore scientifico del Centro di servizio
II	28		Centro di Ateneo e relativi organi
III			**Attività didattica, di ricerca, programmazione e sviluppo**
III	1		Corsi di studio
III	2		Corsi di specializzazione
III	3		Dottorati di ricerca
III	4		Corsi di perfezionamento e di formazione permanente
III	5		Rapporti con enti, istituti di area socio-sanitaria, aziende ed imprese
III	6		Accordi di ricerca e scambi culturali con l'Italia e con l'estero
III	7		Cooperazione con paesi in via di sviluppo
III	8		Piani di sviluppo dell'Università
III	9		Ordinamento Didattico
III	10		Master
III	11		Corsi ad ordinamento speciale
III	12		Strategie e valutazione della didattica e della ricerca
III	13		Premi e borse di studio finalizzati e vincolati
III	14		Opere dell'ingegno e imprenditoria della ricerca
III	15		Progetti e finanziamenti
III	16		Programmi di mobilità
III	17		Programmazione didattica, orario delle lezioni, gestione delle aule e degli spazi
III	18		Gestione di esami di profitto, di laurea e di prove di idoneità
III	19		Programmazione e sviluppo, comprese aree, macroaree e settori scientifico-disciplinari
III	20		Collaborazioni esterne (cultori della materia, visiting professor)
III	21		Convenzioni ed attività per conto terzi
III	22		Assegni di ricerca
IV			**Affari Legali**
IV	1		Contenzioso giudiziale e stragiudiziale
IV	2		Atti di liberalità
IV	3		Reati e contravvenzioni
IV	4		Responsabilità civile, penale ed amministrativa del personale
IV	5		Pareri e consulenze
V			**Studenti e Laureati**
V	1		Orientamento, informazione e tutorato
V	2		Immatricolazioni
V	3		Passaggi interni e trasferimenti da e per altra sede
V	4		Cursus Studiorum e provvedimenti disciplinari
V	5		Diritto allo studio, assicurazioni, benefici economici, tasse e contributi
V	6		Cessazione o conclusione carriera di studio
V	7		Esami di Stato ed ordini professionali
V	8		Tirocinio, programmi di formazione e ricerca
V	9		Progetti speciali
V	10		Servizi di assistenza
V	11		Premi e borse di studio Post-Lauream

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

TITOLO	CLASSE		DESCRIZIONE
V	12		Associazionismo, goliardia e manifestazioni organizzate da studenti o ex studenti
VI			**Strutture didattiche, di ricerca e di servizio**
VI	1		Poli
VI	2		Facoltà
VI	3		Dipartimenti
VI	4		Scuole di specializzazione
VI	5		Centri
VI	6		Biblioteche e sistema bibliotecario
VI	7		Musei, pinacoteche e collezioni scientifiche
VI	8		Consorzi ed enti a partecipazione universitaria
VI	9		Scuole di Dottorato
VI	10		Strutture ad ordinamento speciale
VII			**Personale docente**
VII	1		Concorsi
VII	2		Assunzioni e cessazioni
VII	3		Comandi e distacchi
VII	4		Contratti, Supplenze ed Autorizzazioni per incarichi esterni
VII	5		Carriera
VII	6		Retribuzione e compensi
VII	7		Adempimenti fiscali, contributivi ed assicurativi
VII	8		Pre-ruolo, trattamento di quiescenza, buonuscita
VII	9		Dichiarazioni di infermità, infortunio ed equo indennizzo
VII	10		Servizi a domanda individuale
VII	11		Assenze
VII	12		Tutela della salute e sorveglianza sanitaria
VII	13		Giudizi di merito e provvedimenti disciplinari
VII	14		Deontologia professionale ed etica del lavoro
VIII			**Personale tecnico amministrativo**
VIII	1		Concorsi e selezioni
VIII	2		Assunzioni e cessazioni
VIII	3		Comandi e distacchi
VIII	4		Incarichi
VIII	5		Gestione carriera del dipendente e trattamento economico fondamentale
VIII	6		Compensi accessori scaturenti dal contratto collettivo integrativo
VIII	7		Adempimenti fiscali, contributivi ed assicurativi
VIII	8		Pre-ruolo, trattamento di quiescenza, buonuscita
VIII	9		Dichiarazioni di infermità infortunio ed equo indennizzo
VIII	10		Servizi a domanda individuale
VIII	11		Assenze
VIII	12		Tutela della salute e sorveglianza sanitaria
VIII	13		Provvedimenti disciplinari
VIII	14		Formazione professionale
VIII	15		Personale non strutturato
VIII	16		Orario di lavoro
VIII	17		Deontologia professionale ed etica del lavoro
IX			**Finanza, contabilità e bilancio**

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

TITOLO	CLASSE		DESCRIZIONE
IX	1		Entrate
IX	2		Uscite per la didattica e la ricerca scientifica
IX	3		Uscite per i servizi generali e tecnico-amministrativi
IX	4		Rendicontazioni
IX	5		Bilancio preventivo, rendiconto consuntivo e verifiche contabili
IX	6		Tesoreria, cassa ed istituti di credito
IX	7		Imposte, tasse, ritenute previdenziali ed assistenziali
IX	8		Fondo comune di Ateneo
X			**Lavori pubblici, edilizia ed impiantistica**
X	1		Progettazione e costruzione di nuove opere edilizie con relativi impianti
X	2		Manutenzione ordinaria, straordinaria, ristrutturazione, restauro e destinazione d'uso
X	3		Sicurezza e messa a norma degli ambienti di lavoro
X	4		Telefonia, telematica ed informatica
X	5		Programmazione territoriale
X	6		Materiali, attrezzature tecniche ed adempimenti tecnico-normativi
XI			**Patrimonio, provveditorato ed economato**
XI	1		Acquisizione di beni immobili e relativi servizi
XI	2		Locazione di beni immobili, di beni mobili e relativi servizi
XI	3		Acquisizione e fornitura di beni mobili, di materiali e attrezzature non tecniche e di servizi
XI	4		Manutenzione di beni mobili
XI	5		Alienazione di beni immobili e di beni mobili
XI	6		Ecologia
XI	7		Pagamenti, rimborsi, fondo piccole spese
XI	8		Inventario, rendiconto patrimoniale, beni in comodato
XI	9		Partecipazioni e investimenti finanziari
XI	10		Tutela e valorizzazione dei beni culturali
XII			**Oggetti diversi**
XII	1		Generico

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A13. REPERTORI GENERALI

Di seguito si riporta elenco dei repertori utilizzati nell'Amministrazione:

- Decreti rettoriali
- Decreti direttorali
- Decreti dirigenziali
- Ordini di Servizio
- Atti legali notificati
- Atti legali notificati – Contenzioso del lavoro
- Verbali digitali di esame
- Estratti omissis delibere OO. CC.
- Gare
- Ordinativi Informatici
- Iter autorizzazione decreti
- Verbali Comitato Direttivo CSI
- Estratti omissis delibere CSI

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

A14. ELEMENTI DELLA SEGNATURA DI PROTOCOLLO PER LA CORRISPONDENZA CARTACEA

A14.1 Esempio di segnatura prodotta dagli scanner massivi

Di seguito, si riporta un esempio di segnatura di documento in arrivo, apposta da uno scanner presso l'Ufficio Protocollo dell'Amministrazione Centrale.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

28/09/2012 0101106 UNINA FEDII
data numero di protocollo

posizione Segr. D.G.

Tit. I/6

Al Direttore Tecnico dell'Area
E-Government c/o CSI
dott.ssa Clelia Baldo

Al Capo dell'Ufficio
Protocollo e Archivio

LORO SEDI

OGGETTO: PG 99695 del 25.09.2012. Stati generali della cultura. Trasmissione per adempimenti di competenza.

Si trasmette, in allegato, il documento in oggetto, con il quale l'Associazione

A14.2 Esempio di segnatura prodotta dagli scanner presso le UOR diverse dall'amministrazione Centrale

Di seguito si riporta l'immagine di una etichetta adesiva utilizzata come timbro di arrivo della corrispondenza cartacea in ingresso nelle UOR diverse dalla Amministrazione Centrale.

Gli elementi della segnatura risultano evidenti:

- Codice AOO ovvero Università degli Studi di Napoli Federico II,
- denominazione UOR a cui afferisce la UOP protocollante,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

- numero di protocollo composto dall'anno e dal progressivo nell'anno completo di zeri non significativi,
- giorno, mese e anno,
- orario (facoltativo),
- codice a barre in cui è riportato quanto scritto in chiaro.

La presenza del codice a barre consente che, dalle postazioni abilitate possa essere effettuata - a valle della registrazione dei metadati della corrispondenza in arrivo, in partenza o tra uffici - l'acquisizione per lotti dei documenti protocollati, con la contestuale associazione automatica tra le registrazioni e le rispettive immagini. In questo caso, l'etichetta svolge il compito di "separatore" tra un documento ed il successivo. E' prevista nel breve periodo la migrazione di questo componente integrato nel sistema del protocollo, attualmente basato su librerie di tipo proprietario per la gestione delle immagini, in ambiente open source.

A14.3 Il timbro digitale

Con timbro digitale si intende, secondo la definizione data dall'Agenzia per l'Italia Digitale, un contrassegno, cioè una rappresentazione convenzionale di informazioni contenute nel documento elettronico (tutte o parte di esse), stampabile, riconoscibile con strumenti elettronici, ottenuta utilizzando una codifica grafica definita.

Il timbro digitale rappresenta ad oggi una delle tecnologie più interessanti in grado di rendere indipendente l'autenticità del documento dal supporto utilizzato.
La tecnologia dei timbri digitali si basa fondamentalmente sui codici grafici bidimensionali e cioè su di una rappresentazione di informazioni in formato visivo su una superficie piana (supporto cartaceo, lastra di silicio, ecc.). Tipicamente, un codice bidimensionale si presenta come una matrice di elementi quadrangolari bianchi e neri; tali elementi, detti moduli, sono atti a codificare l'informazione secondo la simbologia prescelta. Per simbologia si intende l'insieme delle regole che definiscono il mapping fra il messaggio e la rispettiva rappresentazione sotto forma di codice grafico.

Concettualmente, in analogia a un codice a barre, un codice bidimensionale è un vettore di informazioni; tuttavia, a differenza di quanto avviene in un codice a barre, la codifica delle informazioni si articola in due dimensioni.; coinvolge sia la dimensione

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013

orizzontale che quella verticale del simbolo, a tutto vantaggio della capacità di memorizzazione.

Con l'utilizzo di una simbologia bidimensionale ad alta densità di memorizzazione è possibile codificare tutto il documento elettronico di partenza, completo di firma, all'interno di uno o più simboli da apporre sulle aree sgombre del documento. ed acquisirlo, a partire dal codice grafico, in una successiva fase del ciclo di vita del documento, In tal modo, la sottoscrizione elettronica iniziale resta valida e verificabile a prescindere dal mezzo di memorizzazione.

Le codifiche attualmente disponibili per i timbri digitali, sono circa una ventina, ma tra le più diffuse vi è la PDF417 che è quella scelta per l'applicazione del timbro digitale in quanto approvata come standard ISO/IEC, diffusa in modalità Open source sia in codifica che in decodifica, consente una scansione anche non esattamente in orizzontale, ha una capienza maggiore rispetto ad altre codifiche (fino a 2710 cifre oppure 1850 caratteri alfanumerici).

Di seguito, un esempio di contrassegno elettronico apposto su documenti informatici sottoscritti digitalmente e registrati nel PdP:

Universita' di Napoli Federico II
UOR: UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II
Data: 13/11/2008, PG/2008/0001415
Firmatari: CLELIA BALDO

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SEGRETERIA DIREZIONE GENERALE
allegato al DG/2013/1503 del 15/11/2013