UNIVERSITÀ DEL SALENTO

PROGETTO S.I.G.D.

LINEE GUIDA PER L'AVVIO DELLE FUNZIONALITÀ INTEROPERATIVE

Titolo: Linee guida Interoperabilità

Gruppo di lavoro:

De Giorgi Valeria	- Dipartimento di Studi Aziendali, Giuridici ed Ambientali
Giannelli Maria Ida	- Direzione Amministrativa – Ufficio Affari legali e Convenzioni
Longo Christian	- Facoltà di Lettere e Filosofia
Marra Antonio	- Dipartimento innovazione e sviluppo – Ufficio Servizi Informatici
Pedaci Piero	- Dipartimento di Studi Giuridici
Rizzo Anna Rita	- Facoltà di Giurisprudenza
Solidoro Sebastiano (*Coordinatore)*	Direzione Amministrativa - Ufficio Documentazione e Archivi
Solombrino Mariacristina	- Facoltà di Lingue e Letterature Straniere
Solombrino Paola	- Dipartimento di Ingegneria dell'Innovazione
Venneri Anna Rita	- Scuola Superiore Isufi

Natura e finalità del documento

Il presente documento, prodotto dal Gruppo di lavoro istituito con nota del Direttore Amministrativo del 3 dicembre 2007 prot. n. 50684, è finalizzato “alla definizione dell'impianto regolamentare per l'avvio delle funzionalità interoperative” tra le Aree Organizzative Omogenee dell'Ateneo.
In conformità al mandato ricevuto dal Gruppo di lavoro, le linee di regolamentazione qui tratteggiate si riferiscono ai flussi documentali interni all'Università del Salento.
L'auspicabile estensione dell'interoperabilità verso PP.AA. esterne ed altri soggetti dovrà formare oggetto di apposite attività deliberative, progettuali e regolamentari.

Introduzione

Il protocollo informatico nasce dall'esigenza di migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei, e attraverso la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali.
Il protocollo informatico è stato implementato nell'Università del Salento attraverso il progetto S.I.G.D. (Sistema Informativo Gestione Documentale) e si è concretizzato nell'adozione e nell'implementazione del sistema software Titulus per la gestione dei flussi documentali e del protocollo.
Con il termine **interoperabilità** si definiscono le funzionalità di trattamento automatico, da parte di un sistema di protocollo informatico ricevente, delle informazioni trasmesse da un sistema di protocollo informatico mittente, allo scopo di automatizzare le attività ed i procedimenti amministrativi conseguenti. Il CNIPA ha emanato un insieme di norme tecniche che stabiliscono nel complesso il protocollo di comunicazione da adottare da parte dei sistemi informatici al fine di poter interscambiare i documenti protocollati. L'interoperabilità utilizza la *posta elettronica certificata* (PEC) per la comunicazione tra i sistemi, per garantire la *sicurezza* e la *non ripudiabilità* della comunicazione. Ogni messaggio di posta elettronica generato per l'interoperabilità contiene le informazioni circa il documento protocollato trasmesso, opportunamente codificate in XML, sempre secondo quanto stabilito dalle norme tecniche del CNIPA.
Il sistema Titulus rispetta le norme tecniche del CNIPA in materia di interoperabilità e pertanto consente, se opportunamente configurato, di scambiare le registrazioni di protocollo con altri sistemi di protocollo informatico di altri Enti o, all'interno dello stesso Ente, tra le diverse Aree Organizzative Omogenee che lo compongono.
In seguito a un'opportuna fase di test, tutte le comunicazioni tra le diverse AOO dell'Università avvengono utilizzando le funzioni di interoperabilità di Titulus.
Alle caselle di posta elettronica dell'Università possono pervenire le seguenti tipologie di documenti informatici:

- documenti sottoscritti mediante firma digitale;
- documenti con firma elettronica e documenti con firma elettronica avanzata;
- documenti sottoscritti da autori identificati mediante l'uso della carta d'identità elettronica o carta nazionale dei servizi;
- documenti trasmessi da altre P.A. e conformi alle direttive relative alla interoperabilità;
- documenti elettronici generici.

I documenti informatici che pervengono alla casella di posta elettronica certificata sono trattati dall'Ufficio/Servizio Protocollo con le medesime procedure usate per i documenti cartacei (registrazione a protocollo, classificazione, smistamento, assegnazione, fascicolazione).
L'Ufficio/Servizio Protocollo, dotato dei dispositivi atti ad accertare l'autenticità e l'integrità del documento, procede alla registrazione dello stesso documento.

Titolo I – Disposizioni Generali

Definizioni

Agli effetti delle Linee Guida si intendono per:

a) «interoperabilità in Titulus»: interscambio di documenti protocollati con altre Aree Organizzative Omogenee attraverso il sistema di gestione documentale Titulus;
b) «posta elettronica certificata»: sistema di posta elettronica nel quale è fornito al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;
c) «atto amministrativo»: qualunque manifestazione di volontà di conoscenza o di giudizio o di natura mista avente rilevanza esterna, posta in essere da un'autorità amministrativa nell'esercizio di una funzione amministrativa per un caso concreto e per destinatari determinati o determinabili;
d) «documento informatico»: rappresentazione informatica del contenuto di atti, fatti o dati giuridicamente rilevanti;
e) «documento analogico»: documento formato utilizzando una grandezza fisica che assume valori continui, come, ad es., le tracce su carta, le immagini formate su un supporto fotografico, o comunque codificato su supporti tradizionali senza l'ausilio di tecnologie informatiche;
f) «soggetti abilitati»: strutture che gestiscono l'interoperabilità in titulus, corrispondente ad ogni AOO;
g) «utente»: la persona fisica che agisce all'interno delle AOO;
h) «attori»: le Aree Organizzative Omogenee e le Unità Organizzative dell'amministrazione; tali aree ed unità compongono, nel loro complesso, la struttura di funzionamento dell'Università come definita dal Manuale di Gestione del S.I.G.D. approvato giusta Decreto del Direttore Amministrativo n. 3 del 13.01.2005.

Campo di Applicazione

1. Le presenti Linee guida sono adottate ai sensi della Direttiva Presidenza Consiglio dei Ministri 27 novembre 2003 – *Impiego della posta elettronica nelle Pubbliche Amministrazioni*, del D.P.R. 11 febbraio 2005, n. 68 *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della Legge 16 gennaio 2003, n. 3* e del D.Lgs. 7 marzo 2005, n. 82 - *Codice dell'Amministrazione Digitale* come successivamente modificato ed integrato con il D.Lgs. n. 159 del 4 aprile 2006.
2. Salvo quanto previsto dall'art. 3, comma 1, del D.Lgs. n. 196/2003: "*I sistemi informatici e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*", le presenti linee guida descrivono le attività finalizzate ad una corretta registrazione di protocollo dei documenti e ad una conseguente corretta modalità di trasmissione degli stessi, al fine di una più efficiente gestione del flusso informativo e documentale interno dell'Università del Salento, dello snellimento delle procedure, della trasparenza dell'azione amministrativa e di una riduzione della spesa, sia in termini di risparmi diretti (carta, spazi) sia di risparmi indiretti (tempo, efficienza).

Riferimenti normativi e giurisprudenziali

- Legge 7 agosto 1990, n. 241 - *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*;
- Legge 15 maggio 1997, n. 127 – *Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo*;
- D.P.R. 10 novembre 1997, n. 513 - *Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;*
- Autorità per l'informatica nella Pubblica Amministrazione, Deliberazione 30 luglio 1998, n. 24/98 - *Regole tecniche per l'uso di supporti ottici*;
- D.P.R. 20 ottobre 1998, n. 428 - *Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche;*
- Raccomandazione CE 23 gennaio 1999, n. 1 - *Trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware;*
- D.P.C.M. 8 febbraio 1999 - *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513*;
- D.P.C.M. 28 ottobre 1999 - *Gestione informatica dei flussi documentali nelle pubbliche amministrazioni;*
- Direttiva 13 dicembre 1999, n. 1999/93/CE - *relativa ad un quadro comunitario per le firme elettroniche;*
- D.P.C.M. 31 ottobre 2000 - *Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998, n. 428;*
- 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;*
- D.P.R. 28 dicembre 2000, n. 445 - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
- D.Lgs. 30 marzo 2001, n. 165 - *Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*;
- Circolare AIPA 7 maggio 2001, n. 28 - *Regole tecniche per il protocollo informatico di cui al D.P.R. 28.12.2000, n. 445 – Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati;*
- Circolare AIPA 21 giugno 2001, n. 31 - *Requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente*;
- Deliberazione AIPA 13 dicembre 2001, n. 42 - *Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali – articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al D.P.R. 28 dicembre 2000, n. 445;*
- Direttiva Ministeriale 21 dicembre 2001 - *Linee guida in materia di digitalizzazione dell'amministrazione;*
- D.Lgs. 23 gennaio 2002, n. 10 - *Attuazione delle direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*;
- Direttiva Ministeriale 9 dicembre 2002 - *Trasparenza dell'azione amministrativa e gestione dei flussi documentali;*
- D.P.R. 7 aprile 2003, n. 137 - *Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'art. 13 del D.Lgs. n. 10/2002*;

- D.Lgs. 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali;*
- Direttiva Presidenza Consiglio dei Ministri 27 novembre 2003 – *Impiego della posta elettronica nelle Pubbliche Amministrazioni*
- D.Lgs. 22 gennaio 2004, n. 42 – *Codice dei beni culturali e del paesaggio*
- 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 – Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al D.P.R. 28 dicembre 2000, n. 445;*
- Legge 11 febbraio 2005, n. 15 - *Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernente norme generali sull'azione amministrativa*;
- D.P.R. 11 febbraio 2005, n. 68 - *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della Legge 16 gennaio 2003, n. 3;*
- D.Lgs. 28 febbraio 2005, n. 42 - *Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229;*
- D.Lgs. 7 marzo 2005, n. 82 - *Codice dell'Amministrazione Digitale;*
- D.M. 2 novembre 2005 - *Regole tecniche per la formazione, la trasmissione e validazione, anche temporale, della posta elettronica certificata*;
- Direttiva Presidenza Consiglio dei Ministri 18 novembre 2005 - *Linee guida per la Pubblica amministrazione digitale*;
- D.Lgs. 4 aprile 2006, n. 159 – *Modifiche ed integrazioni al Codice dell'Amministrazione Digitale*;
- D.P.R. 12 aprile 2006, n. 184 – *Regolamento di disciplina in materia di accesso ai documenti amministrativi;*
- Legge 24 dicembre 2007, n. 244 (legge finanziaria 2008);
- Sentenza della Cassazione Civile – sez. Lavoro – del 6 settembre 2001 n. 11445;
- Decreto ingiuntivo emesso dal Tribunale di Cuneo – sez. civile - l'11.12.2003;
- Parere del Consiglio di Stato n. 11995 del 7.02.2005;
- Sentenza TAR Calabria del 9.02.2005;
- Ordinanza del 2.06.2005 del Tribunale Ordinario di Bari – sez. IV Civile.

Normativa interna

- Statuto dell'Università del Salento;
- Manuale di Gestione del Sistema Informativo Gestione Documentale (S.I.G.D.);
- Circolare del Direttore Amministrativo prot. n. 47391 del 19.11.2007 – *Circolare sulla trasmissione dei documenti*;
- Circolare del Direttore del Dipartimento Innovazione e Sviluppo prot. n. 50868 del 4/12/2007 – *Sistema di gestione documentale Titulus – Rispetto degli standard tecnici e delle linee guida per l'inserimento dei dati*.

Titolo II – Aree Organizzative Omogenee (AOO) e Unità Organizzative (UO)

Soggetti abilitati

Ogni AOO è dotata di una casella di posta elettronica certificata attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità dell'Ufficio/Servizio di Protocollo; l'Ufficio/Servizio procede alla lettura della corrispondenza ivi pervenuta e adotta quanto previsto in relazione alle varie tipologie di messaggi.
L' Unità Organizzativa è l'Ufficio (sezione, settore etc.) attraverso il quale si articola in livelli gerarchici la struttura di un'Area Organizzativa Omogenea che ne utilizza i servizi messi a disposizione per la gestione dei documenti.
Ogni AOO è un'insieme di unità organizzative che dal punto di vista amministrativo e contabile svolgono in modo omogeneo le attività della Struttura di riferimento.
Nei casi e alle condizioni stabilite dallo Statuto dell'Università del Salento, i soggetti abilitati all'utilizzo della Posta elettronica certificata sono individuati sulla base della seguente suddivisione:

AOO	*Casella PEC*	*Userid*
Amministrazione centrale	amministrazione.centrale@cert-unile.it	KLD00002
Centro cultura innovativa d'impresa	centro.cultura.innovativa.impresa@cert-unile.it	KLD00003
Centro linguistico di ateneo	centro.linguistico.ateneo@cert-unile.it	KLD00004
Dipartimento dei beni delle arti e della storia	dip.beni.arti.storia@cert-unile.it	KLD00005
Dipartimento di beni culturali	dip.beni.culturali@cert-unile.it	KLD00006
Dipartimento di filologia classica e scienze filosofiche	dip.filologia.classica@cert-unile.it	KLD00007
Dipartimento di filologia linguistica e letteratura	dip.filologia.linguistica@cert-unile.it	KLD00008
Dipartimento di filosofia e scienze sociali	dip.filosofia.scienze.sociali@cert-unile.it	KLD00009
Dipartimento di fisica	dip.fisica@cert-unile.it	KLD00010
Dipartimento di ingegneria dell'innovazione	dip.ingegneria.innovazione@cert-unile.it	KXX0008
Dipartimento di lingue e letterature straniere	dip.lingue.letterature.straniere@cert-unile.it	KLD00011
Dipartimento di matematica 'Ennio De Giorgi'	dip.matematica@cert-unile.it	KLD00012
Dipartimento di scienze economiche e matematico-statistiche	dip.scienze.economiche@cert-unile.it	KLD00015
Dipartimento di scienza dei materiali	dip.scienze.materiali@cert-unile.it	KLD00013
Dipartimento di scienze pedagogiche	dip.scienze.pedagogiche@cert-unile.it	KLD00016
Dipartimento di scienze sociali e della comunicazione	dip.scienze.sociali.comunicazione@cert-unile.it	KLD00017
Dipartimento di scienze e tecnologie biologiche ed ambientali	dip.scienze.tecnologie.biologiche@cert-unile.it	KLD00014
Dipartimento di studi aziendali	dip.studi.aziendali@cert-unile.it	KLD00018
Dipartimento di studi giuridici	dip.studi.giuridici@cert-unile.it	KXX0006
Dipartimento di studi storici dal medioevo all'età contemporanea	dip.studi.storici@cert-unile.it	KLD00019
Facoltà di beni culturali	fac.beni.culturali@cert-unile.it	KLD00020
Facoltà di economia 'Antonio De Viti De Marco'	fac.economia@cert-unile.it	KXX0007
Facoltà di giurisprudenza	fac.giurisprudenza@cert-unile.it	KLD00021
Facoltà di ingegneria industriale	fac.ingegneria.industriale@cert-unile.it	KLD00023
Facoltà di ingegneria	fac.ingegneria@cert-unile.it	KLD00022
Facoltà di lettere e filosofia	fac.lettere.filosofia@cert-unile.it	KLD00024

Facoltà di lingue e letterature straniere	fac.lingue.letterature.straniere@cert-unile.it	KLD00025
Facoltà di Scienze della formazione	fac.scienze.formazione@cert-unile.it	KLD00026
Facoltà di scienze matematiche fisiche e naturali	fac.scienze.mmffnn@cert-unile.it	KLD00027
Facoltà di scienze sociali, politiche e del territorio	fac.scienze.sociali.politiche.territorio@cert-unile.it	KLD00029
Scuola superiore ISUFI	scuola.superiore.isufi@cert-unile.it	KLD00028

Ciascuna AOO individua autonomamente le proprie esigenze di articolazione interna ai fini della gestione dei flussi documentali, valutando la possibilità di ricorrere alla istituzione di Unità Organizzative (ad es. Consigli Didattici, Centri, Servizi, Biblioteche).
Qualora risulti necessario, il responsabile della AOO richiede all'Amministrazione Centrale l'istituzione delle UO nell'ambito del sistema Titulus, indicando le unità di personale che vi afferiscono.

Titolo III - Descrizione funzionale del sistema di posta elettronica certificata e delle funzioni di interoperabilità in Titulus

La Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata è una evoluzione del servizio di posta elettronica tradizionale che consente la piena tracciabilità del messaggio, la sicurezza della trasmissione e la non ripudiabilità quando questo intercorra tra due caselle PEC. La trasmissione di un messaggio o di un documento tramite PEC è valida agli effetti di legge.
Il DPR 11 febbraio 2005, n. 68 disciplina le modalità di utilizzo della PEC nei rapporti tra e con la Pubblica Amministrazione e privati cittadini. Il CNIPA ha emanato conseguentemente le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" in cui sono dettagliati tutti i requisiti tecnico-funzionali. Il citato DPR 68 stabilisce altresì che i gestori di caselle PEC devono essere accreditati presso il CNIPA, subordinatamente al rispetto dei requisiti richiesti. Per ulteriori informazioni si veda *http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Posta_Elettronica_Certificata__(PEC)/*

Il funzionamento della PEC

Si riassume schematicamente il funzionamento della trasmissione di un messaggio di PEC:

1) Il mittente compone il messaggio attraverso un client e-mail standard opportunamente configurato (anche una applicazione webmail) e lo trasmette al proprio gestore PEC;
2) Il gestore PEC prende in carico il messaggio e ritorna al mittente un messaggio di riscontro (di accettazione) dell'avvenuta presa in carico del messaggio in uscita;
3) Il gestore PEC mittente invia il messaggio al gestore PEC destinatario. Il gestore PEC destinatario invia un riscontro al gestore PEC mittente dell'avvenuta presa in consegna (o del rifiuto) del messaggio;
4) Il gestore PEC mittente invia al mittente originale del messaggio un riscontro di avvenuta consegna, che attesta che il destinatario ha disponibile il messaggio inviato nella propria casella PEC, anche se non lo ha ancora letto (o la segnalazione di una eccezione).

Le eccezioni che vengono gestite in caso di problemi nella consegna del messaggio sono:

1) la non accettazione (ad es. in caso di presenza di virus o destinatari in copia nascosta – non ammessi per le PEC -, ecc.)
2) la mancata consegna (in caso di problemi di rete o altro)
3) la rilevazione di virus informatici nel messaggio.

La comunicazione avviene sempre mediante protocolli sicuri (SMTPS per l'invio, POP3S o IMAPS per lo scarico dei messaggi). L'onere della garanzia della tracciabilità dei messaggi di posta elettronica certificata grava quindi sui gestori coinvolti (mittente e destinatario); il CNIPA svolge l'attività di controllo sull'operato dei gestori accreditati.
Una casella PEC può ricevere anche messaggi di posta elettronica non certificata, ma in questo caso il messaggio viene segnalato come anomalo (sebbene rimanga perfettamente leggibile dal destinatario).

Il gestore PEC dell'Ateneo

L'Università del Salento ha attivato 31 caselle PEC, una per ogni AOO individuata, presso un gestore accreditato CNIPA. Nella fattispecie si tratta di InfoCert S.p.A. (nuova società emanazione di Infocamere – il precedente gestore - ed accreditata presso il CNIPA dal 19.7.2007), che fornisce il servizio attraverso il prodotto LegalMail (http://www.legalmail.it). Per garantire la corretta fruizione del servizio attraverso un dominio e-mail riconoscibile, è stato registrato il dominio cert-unile.it, in quanto per una incompatibilità tecnica dei server DNS del GARR non è possibile appoggiarsi al dominio unile.it proprio dell'Università del Salento.
Il servizio Legalmail è accessibile attraverso una interfaccia Web, ma è possibile configurare un qualsiasi client e-mail recente (ad es. Mozilla Thunderbird, Microsoft Outlook e Outlook Express) che supporti i protocolli sicuri POP3S o IMAPS per la ricezione e SMTPS per la trasmissione. L'accesso sicuro alla casella PEC, sia via webmail che attraverso un client dedicato, viene autenticato attraverso un certificato autoprodotto da Infocamere.

Le funzioni di interoperabilità

L'interoperabilità consente, dopo la protocollazione in uscita di un documento, di inviare telematicamente lo stesso all'AOO destinataria attraverso un messaggio di PEC opportunamente formato e contenente sia i metadati della registrazione che la scansione e gli allegati informatici. Requisiti fondamentali sono quindi che la AOO destinataria sia dotata di una casella PEC di cui sia noto l'indirizzo e-mail e che tale casella sia gestita anche attraverso un sistema di protocollazione elettronica che risponda ai requisiti dettati dalle norme tecniche CNIPA.
Titulus implementa le funzioni di interoperabilità e consente quindi di ricevere documenti protocollati da altre AOO direttamente in formato elettronico, completi di scansioni e/o allegati, creando una bozza di documento che può essere protocollata, smistata ad altro utente, conservata come documento non protocollato o scartata dalla AOO ricevente.
La protocollazione della bozza, in particolare, si attiva con un solo click sul pulsante "Protocolla" che appare nella visualizzazione della bozza stessa (dopo aver ovviamente integrato o adeguato i dati del documento, quali ad es. la classificazione). Il documento, protocollato o no, può quindi essere smistato ad altri utenti Titulus attraverso le classiche operazioni di "Nuovo RPA" e "Nuovo CC".
Le funzioni di interoperabilità previste da Titulus consentono una notevole efficienza nella gestione documentale dell'Ateneo, riducendo al minimo la duplicazione del lavoro tra la protocollazione in uscita del mittente e quella in entrata del destinatario.
Titulus si configura sia come mittente che destinatario dei messaggi PEC di interoperabilità:

1) come mittente nella fase di protocollazione in partenza, laddove il documento protocollato in partenza sia destinato ad una struttura esterna la cui registrazione in anagrafica comprende l'indicazione dell'indirizzo di PEC associato alla struttura destinataria;

2) come destinatario dei messaggi PEC di interoperabilità in arrivo sulla casella PEC configurata per ciascuna AOO dell'Ateneo.

Affinché nella protocollazione in partenza sia data la possibilità all'utente di inviare telematicamente il documento è necessario che l'anagrafica della struttura (o della persona) destinataria comprenda l'indirizzo PEC relativo alla AOO ad essa associata. In tal caso Titulus, completata la protocollazione del documento, fa apparire accanto all'indicazione del destinatario l'icona di una bustina bianca, cliccando sulla quale si effettua l'invio telematico del documento.
A tal proposito si è proceduto ad una "bonifica" delle anagrafiche esterne relative ad AOO o UO dell'Università del Salento registrate dagli utenti nel sistema attraverso la rimozione dei duplicati riscontrati e alla normalizzazione delle registrazioni secondo quanto dettato dalle "Linee guida

per l’inserimento e l’aggiornamento di anagrafiche nel protocollo informatico”, allegate all’”Avvio operativo del S.I.G.D. (Sistema Informativo Gestione Documentale)” pubblicato sul sito del Dipartimento Innovazione e Sviluppo. Si è quindi proceduto ad integrare tali anagrafiche con l’indicazione dell’indirizzo PEC associato alla AOO di appartenenza della struttura.
Si raccomanda di non modificare le anagrafiche esterne relative a strutture dell’Università del Salento (sia AOO che UO) per non pregiudicare la corretta attivazione delle funzioni di interoperabilità e di fare riferimento, in caso di necessità, all’Ufficio Documentazione e Archivi dell’Amministrazione Centrale.
Titulus provvede inoltre a ricevere e ad allegare al documento tutte le ricevute di accettazione/consegna ecc. previste dal protocollo di PEC.
Una volta che si è effettuato l’invio telematico del documento protocollato è sempre possibile, previa ulteriore conferma, effettuare nuovamente l’invio del documento con le stesse modalità già illustrate.
Presso la AOO destinataria il documento viene ricevuto come bozza completa di allegati informatici e scansioni del documento, con anche l’indicazione del numero di protocollo assegnato dal mittente. Il protocollista della AOO ricevente (o il suo responsabile di protocollo) provvede quindi a protocollare la bozza attraverso un click su un pulsante “Protocolla” o a registrarlo come documento non protocollato (se non è prevista la protocollazione), dopo aver eventualmente adeguato i metadati associati alla registrazione. E’ altresì possibile inviare la bozza ad un altro utente del sistema (in RPA o in CC) delegando così la valutazione e/o la protocollazione del documento in arrivo ad un’altra persona.
In questo caso Titulus agisce come destinatario del messaggio PEC. A tal scopo le caselle PEC relative alle AOO sono appositamente registrate e configurate in Titulus. Le informazioni registrate sono complete di tutti i dati necessari per consentire a Titulus sia l’invio che la ricezione di messaggi attraverso la casella PEC, compresa la password dell’account PEC. Il sistema provvede, ogni 600 secondi (10 minuti) ad effettuare il polling (interrogazione ciclica) delle caselle PEC registrate per scaricare i messaggi relativi all’interoperabilità con i relativi riscontri, lasciando sul server PEC tutti i messaggi non di interoperabilità.
Ciascuna AOO garantisce il presidio della corrispondenza in arrivo tramite PEC, sia con riferimento alla corrispondenza gestita in regime di interoperabilità (cioè quella proveniente da casella PEC di altra AOO dell'Ateneo e automaticamente presa in carico dalla procedura Titulus) sia con riferimento alla corrispondenza non munita degli attributi di interoperabilità.
Nell'ipotesi che l'AOO non provveda a stabilire dette misure, si applicheranno le seguenti regole:

1. Il presidio della corrispondenza in arrivo tramite PEC, rientra nelle competenze dal *Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi*, afferente a ciascuna AOO.
2. L'accesso alla corrispondenza in arrivo tramite PEC (di interoperabilità e non) è curato dal Responsabile del Servizio di cui al precedente paragrafo 1), salvo quanto disposto al seguente paragrafo 3).
3. E' fatta salva la possibilità di consentire l'accesso alla corrispondenza di interoperabilità anche ad altre unità di personale, individuate dal responsabile della struttura.
4. Ove eserciti la facoltà di cui al precedente paragrafo 3), la AOO interessata avrà cura di stabilire regole univoche atte a prevenire duplicazioni o conflitti di attività e/o di risultati.
5. In ordine alle concrete modalità operative, il presidio della corrispondenza in arrivo avente caratteristiche d'interoperabilità si esplica mediante accesso alla procedura Titulus da parte dell'unità di personale individuata ai sensi dei precedenti paragrafi 2) e 3). A tal fine, detta unità di personale, curerà il regolare accesso al sistema Titulus, secondo le credenziali di autenticazione definite dal sistema di amministrazione della procedura.
6. Eseguito l'accesso alla procedura Titulus, l'unità di personale di cui al precedente paragrafo, prende visione dei documenti d'interoperabilità in arrivo e provvede a smistarli, secondo i casi, dopo averli protocollati, oppure, rimettendone la protocollazione al

successivo utente della procedura abilitato ad eseguirla, secondo quanto stabilito dalle disposizioni interne della struttura. Resta salvo il principio di tempestività della registrazione di protocollo, in conformità alla normativa vigente.

7. Il presidio della corrispondenza in arrivo NON avente caratteristiche d'interoperabilità, si esplica mediante scaricamento della posta dalla casella PEC della struttura. A tal fine, l'unità di personale individuata ai sensi dei precedenti paragrafi 2) e 3) curerà il regolare accesso al client di posta elettronica dedicato, appositamente configurato per scaricare dalla PEC i messaggi non di interoperabilità e provvederà a smistarli a chi di competenza. I parametri di configurazione del client di posta elettronica dedicato sono stabiliti dall'amministratore del sistema Titulus. E' fatta salva la possibilità di accedere alla corrispondenza NON di interoperabilità pervenuta alla casella PEC mediante interfaccia webmail.

La validità giuridica e l'efficacia probatoria dei documenti informatici nella disciplina antecedente il D.Lgs. 159/2006

L'art. 21, comma 2, del Codice dell'Amministrazione Digitale prevede che il documento informatico sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'art. 2702 c.c.; conseguentemente l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

Al riguardo si ripercorre l'excursus storico che ha portato all'introduzione di alcune modifiche nel testo del CAD a seguito delle perplessità manifestate in materia dalla maggior parte della dottrina atteso che la semplice firma, seppur validamente apposta su un documento informatico, non consentiva, comunque, che esso soddisfacesse il requisito legale della forma scritta. Ciò in quanto tale presunzione valeva soltanto per i documenti informatici sottoscritti con firma digitale o altra firma elettronica qualifica, ai sensi dell'art. 20 del previgente Codice delle Amministrazione Digitale.

Giova rilevare che nel T.U. 445/2000 al documento informatico privo di qualsivoglia sottoscrizione elettronica veniva riconosciuta proprio l'efficacia probatoria prevista dall'art. 2712 del codice civile, riguardo ai fatti ed alle cose in esso rappresentate.

Il documento informatico sottoscritto con firma elettronica, invece, soddisfaceva il requisito legale della forma scritta, mentre, sul piano probatorio era liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza: da un lato il legislatore prendeva atto delle nuove potenzialità offerte dall'informatica nell'attività di sottoscrizione, dall'altro ne vincolava l'efficacia probatoria ad una valutazione del giudice circa le condizioni "ambientali" di formazione della stessa.

Nel previgente Codice dell'Amministrazione Digitale poi spariva ogni riferimento all'efficacia probatoria del documento informatico non sottoscritto, salvo volerla recuperare per l'appunto nell' art 23, che modifica l'art. 2712 c.c. introducendo tra le riproduzioni che formano piena prova dei fatti e delle cose in esse rappresentate anche le *"riproduzioni informatiche"*. In questo caso il documento informatico sottoscritto con firma elettronica aveva un'efficacia probatoria inferiore rispetto ad uno non sottoscritto.

Nella pratica, pertanto, se si produceva in giudizio un documento munito di firma elettronica semplice (fermo restando il fatto che esso non soddisfaceva il requisito legale della forma scritta) il giudice era investito di una libera valutazione, in ragione delle sue caratteristiche oggettive di qualità e di sicurezza. Attraverso un'interpretazione sistematica dell'art. 21, commi 1 e 2, si comprende che tale valutazione non poteva comunque portare ad attribuire al documento in esame l'efficacia probatoria prevista dall'art 2702 c.c. che invece era riservata al solo documento informatico munito di firma digitale o di altra firma elettronica qualificata.

Se invece si produceva un documento informatico sprovvisto di qualsiasi sottoscrizione esso ben poteva essere considerato come riproduzione informatica di fatti e di cose di cui all'art. 2712 e dunque fare piena prova dei fatti e delle cose rappresentate, se colui contro il quale era prodotto non ne disconosceva la conformità ai fatti o alle cose medesime

Era allora evidente l'esistenza di un problema interpretativo al quale aveva dato una risposta, anche se non in termini fattivi e concreti, il Consiglio di Stato, nel parere reso nell'adunanza del 7 febbraio 2005, con riferimento alla materia di cui trattasi: **"***la scrittura con firma elettronica (non qualificata) non sembrerebbe integrare la scrittura privata non autenticata di cui all'articolo 1350 c.c., anche se gli autori della scrittura non disconoscono la loro firma. Non si comprende come debba essere considerato l'atto con firma elettronica debole non disconosciuta a norma dell'articolo 215 c.p.c. La previsione della libera valutabilità in giudizio, di cui al primo comma dell'articolo 18 sembra contrastare con il principio desumibile dal codice di rito***"**.

Le novità introdotte dal D.Lgs. 159/2006 in materia di validità giuridica ed efficacia probatoria dei documenti informatici

Al fine di riordinare la materia il D.Lgs. n. 159/2006 ha novellato in alcuni articoli il D.Lgs. n. 82/2005 e conseguentemente la disciplina che oggi regola il documento informatico prevista negli artt. 20 e 21 del novellato D.Lgs. è la seguente.

Il documento informatico in conformità alle regole tecniche (art. 71 CAD) è valido e rilevante agli effetti di legge.

L'idoneità del documento informatico a soddisfare la forma scritta prescinde dalla sottoscrizione ed è liberamente valutabile in giudizio tenendo conto delle caratteristiche oggettive del documento ("*qualità, sicurezza, integrità ed immodificabilità*").

Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale e redatto secondo le regole tecniche, soddisfa il requisito della forma scritta quando essa è richiesta a fini contrattuali dalla legge o dalle parti sotto pena di nullità dell'atto e specificatamente nelle ipotesi di cui al comma 1 articolo 1350 del codice civile; in questo caso vi è, quindi, una valutazione ex lege circa il valore giuridico del documento, a cui il giudice resta vincolato.

Quanto al valore probatorio del documento informatico esso trova disciplina nell'art. 21 del CAD.

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

Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha, invece, l'efficacia prevista dall'articolo 2702 del codice civile (scrittura privata), cioè fa piena prova fino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.

Ed infine, il documento informatico senza firma, viene equiparato dal successivo art. 23 – ai fini probatori – alle riproduzioni meccaniche, che – ai sensi dell'art. 2712 codice civile – "*formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".

La validità della trasmissione dei documenti informatici all'interno dell'Amministrazione

Il meccanismo dell'interoperabilità è indipendente dal sistema software utilizzato: è quindi possibile estendere gradualmente l'utilizzo dell'interoperabilità verso altri Enti dotati di sistemi software compatibili.
Tale possibilità è prevista solo dopo l'avvio dell'utilizzo della firma digitale per l'autenticazione dei documenti elettronici (requisito fondamentale per la validità giuridica di un documento elettronico nel caso di corrispondenza tra Enti differenti, v. Codice dell'Amministrazione Digitale - artt.20, 21, 24-25).
In ambito interno, il Codice dell'Amministrazione Digitale, all'art. 34 comma 2, lascia alla discrezionalità delle singole Amministrazioni una eventuale regolamentazione sulla "formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna", rendendo possibile quindi adottare meccanismi più snelli per la gestione dei flussi documentali interni.
Si può quindi utilizzare il meccanismo dell'interoperabilità per evitare la spedizione dei documenti originali cartacei anche senza l'utilizzo della firma digitale, ma solo quando il documento rimarrà esclusivamente all'interno dell'Università del Salento.
Il Codice dell'Amministrazione Digitale attribuisce validità giuridica al meccanismo di interoperabilità interna, dato che (art. 45 - "Valore giuridico della trasmissione") "*i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale*" e la provenienza può essere accertata dato che "*Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore*". L'art. 47 estende la validità della trasmissione informatica tra pubbliche amministrazioni anche "*ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza*". Lo stesso art. 47 al comma 2 punti b, c, d elenca tre situazioni esclusive che, nel procedimento di interoperabilità interna, sono contemporaneamente verificate. D'altro canto l'accesso al sistema Titulus è regolato da credenziali di accesso (username e password) che il CAD riconosce come firme elettroniche, liberamente valutabili in sede di giudizio ma tecnicamente abbastanza solide da poter essere opposte a terzi.
Si ricorda, pertanto, che le credenziali di accesso al sistema Titulus (così come qualsiasi accoppiata username e password che regoli l'accesso ad un sistema informatico/telematico) sono strettamente personali e non devono per nessun motivo essere cedute a terzi, compresi colleghi e superiori di qualsiasi ordine e grado. Qualsiasi comportamento che causi anche indirettamente la conoscenza di tali credenziali a terzi deve essere sanato (ad es. mediante il cambio della password), pena la responsabilità dell'utente interessato (cfr. nota del Direttore del Dipartimento Innovazione e Sviluppo prot. n. 18605 del 31.05.2006).
L'interoperabilità è la prima fase della completa informatizzazione del flusso documentale dell'Ateneo. Tale flusso potrà essere completamente informatizzato quando sarà introdotto l'uso della firma digitale per tutti i responsabili di AOO e UO e siano completamente definite le relative procedure. Il CAD infatti prevede la piena validità dei documenti informatici firmati digitalmente nel rispetto della normativa e delle regole tecniche vigenti.

Titolo IV - Il flusso di lavorazione dei documenti informatici

Ricezione e protocollazione di documenti informatici sulla casella di posta elettronica certificata

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata ed è accessibile solo da parte dell'Ufficio deputato alla protocollazione in arrivo dei documenti.
L'operazione di ricezione dei documenti informatici avviene con modalità conformi alle regole correnti recanti standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.
Qualora il documento ricevuto non sia conforme agli standard previsti dalla normativa vigente ovvero non sia sottoscritto con firma digitale e si renda necessario attribuire efficacia probatoria, esso è inserito nel sistema di gestione documentale con il formato di origine apponendo la dicitura "documento ricevuto via posta elettronica" e successivamente protocollato, smistato, assegnato e gestito.
Ciascuna AOO, esclusa l'Amministrazione Centrale, può richiedere che la protocollazione di documenti in arrivo sia affidata direttamente ad unità in servizio presso UO di II o successivi livelli.

Rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.
La riproduzione dei documenti cartacei in formato immagine è eseguita sulla base dei seguenti criteri:

- sono acquisite le immagini dei documenti integrali aventi formato A4
- qualora il documento abbia formati diversi dal precedente è inserita nel campo Annotazione della registrazione di protocollo la dicitura "non si procede alla scansione del … (indicare la tipologia di documento), in quanto …" (indicare la motivazione).

Sono regolarmente protocollati e riprodotti in formato immagine ma resi riservati i seguenti documenti:

- i certificati medici contenenti diagnosi;
- i documenti contenenti dati giudiziari, ai sensi dell'art. 4, comma 1, lett. e) del D.Lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*" ovvero quei documenti contenenti dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u) del D.P.R. 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 ex articoli 60 e 61 del codice di procedura penale;

- documenti contenenti 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 la vita sessuale di un soggetto;
- altri documenti la cui acquisizione, a giudizio del responsabile del procedimento e/o processo, non è opportuna al fine di tutelare esigenze di riservatezza .

Trasmissione e protocollazione di documenti informatici e relativo flusso

La protocollazione, classificazione, fascicolazione e spedizione di un documento informatico in partenza avviene a cura del responsabile di procedimento amministrativo (RPA) o del responsabile di procedura amministrativa (RP). La spedizione avviene mediante la casella di posta elettronica certificata della AOO direttamente attraverso le funzionalità di Titulus.
Sono acquisite le immagini dei documenti integrali aventi formato A4, mentre sono esclusi dalla digitalizzazione solo quei documenti o allegati per i quali la procedura di scansione risulta impossibile o difficoltosa in ragione del formato (documento rilegato, foglio di carta eccedente il formato A4, pubblicazioni, ecc.) o per il tipo di supporto.
Nei casi in cui, per le ragioni suesposte, non sia possibile digitalizzare integralmente i documenti e gli allegati, è inserita nel campo Annotazione della registrazione di protocollo la dicitura "non si procede alla scansione del … (indicare la tipologia di documento), in quanto …" (indicare la motivazione).
Il documento per il quale non si è proceduto alla digitalizzazione è trasmesso necessariamente in formato analogico cartaceo.

Redazione, registrazione e spedizione di documenti aventi per destinatario un'altra AOO dell'Università

Al fine di limitare il flusso di documenti analogici cartacei fra le AOO e le UO dell'Università, i documenti trasmessi tra le AOO dell'Ateneo attraverso il protocollo informatico, integrato con servizi di interoperabilità, si intendono inviati ai sensi del combinato disposto di cui agli artt. 45 e 47 del Codice dell'Amministrazione Digitale e, pertanto, non è più consentita la loro trasmissione in formato analogico cartaceo.
È consentita la trasmissione di documenti cartacei solo ed esclusivamente nel caso in cui gli stessi debbano essere indispensabilmente acquisiti dall'UO destinataria ai fini del procedimento amministrativo cui si riferiscono, così come previsto nel successivo Titolo V.
Le operazioni di registrazione comprendono la classificazione, l'acquisizione in formato immagine dell'intero documento tramite il processo di scansione e conseguente memorizzazione nel sistema *Titulus*.
Sono esclusi dalla digitalizzazione solo quei documenti o allegati per i quali la procedura di scansione risulta impossibile o difficoltosa in ragione del formato (documento rilegato, foglio di carta eccedente il formato A4, pubblicazioni, ecc.) o per il tipo di supporto.
Nei casi in cui, per le ragioni suesposte, non sia possibile digitalizzare integralmente i documenti e gli allegati, è inserita nel campo Annotazione della registrazione di protocollo la dicitura "non si procede alla scansione del … (indicare la tipologia di documento), in quanto …" (indicare la motivazione).

Il sistema *Titulus* mantiene le registrazioni delle operazioni effettuate dal soggetto abilitato ed a quelle connesse con la PEC.
La produzione di copie conformi analogiche di tali documenti spetta al RPA mittente.
Per i parametri ed i formati da utilizzare per le scansioni e gli allegati informatici si faccia riferimento al successivo paragrafo "*Formati tecnici e parametri di scansione*".

Flusso dei documenti interni o tra uffici (UO)

Al fine di limitare il flusso di documenti analogici cartacei fra le UO di una medesima AOO, i documenti informatici prodotti a seguito della protocollazione e scansione di documenti originali cartacei trasmessi tra le Unità Organizzative interne di ciascuna Area Organizzativa Omogenea sono inoltrati in formato digitale tramite il sistema di protocollo informatico senza procedere all'inoltro dell'originale. Il documento informatico è fascicolato, sia in formato analogico sia in formato digitale, dall'Unità Organizzativa mittente, che è responsabile della conservazione presso la stessa UO. L'Unità Organizzativa destinataria deve procedere, invece, soltanto alla fascicolazione del documento informatico. Il sistema di protocollazione informatica effettua la notifica dell'assegnazione del documento al responsabile di procedura amministrativa mediante posta elettronica e dà contezza dell'avvenuta ricezione e lettura del documento da parte del destinatario oltre a tracciare la storia dell'accesso al singolo documento.
Con l'assegnazione del documento al destinatario, il mittente medesimo è esonerato da ogni responsabilità in ordine al segmento procedimentale in carico al destinatario, salvo i casi di errore, dovuti a colpa o dolo del mittente. Si applica in ogni caso, al riguardo, la disciplina normativa esistente in materia.
Si deve procedere alla trasmissione dei documenti cartacei indicati nell'elenco di cui al titolo V delle presenti Linee Guida nonché degli ulteriori documenti che devono essere indispensabilmente acquisiti, in formato analogico e su richiesta motivata del mittente, dall'UO destinataria ai fini del procedimento amministrativo cui si riferiscono.
Sono esclusi dalla digitalizzazione solo quei documenti o allegati per i quali la procedura di scansione risulta impossibile o difficoltosa in ragione del formato (documento rilegato, foglio di carta eccedente il formato A4, pubblicazioni, ecc.) o per il tipo di supporto.
Nei casi in cui, per le ragioni suesposte, non sia possibile digitalizzare integralmente i documenti e gli allegati, è inserita nel campo Annotazione della registrazione di protocollo la dicitura "non si procede alla scansione del … (indicare la tipologia di documento), in quanto …" (indicare la motivazione).
La produzione di copie conformi analogiche di tali documenti spetta al RPA.
Per i parametri ed i formati da utilizzare per le scansioni e gli allegati informatici si faccia riferimento al successivo paragrafo "*Formati tecnici e parametri di scansione*".

Formati tecnici e parametri di scansione

I documenti protocollati devono contenere la scansione dell'originale analogico ed eventuali file allegati, nel rispetto dei seguenti requisiti:

1. le scansioni dei documenti devono essere effettuate direttamente da Titulus secondo i parametri previsti dal Manuale di Gestione: 200 dpi, 1 bit per pixel "bianco e nero". Nel caso non fosse possibile effettuare la scansione direttamente dall'interno di Titulus, le immagini delle scansioni devono rispettare gli stessi parametri ed essere in formato TIFF Fax CCITT Group 4 (lo stesso utilizzato internamente da Titulus);
2. i file allegati del documento protocollato devono:

1. utilizzare formati standard, accessibili con strumenti di comune reperibilità, gratuiti e/o liberi (*open source*), non legati ad un particolare sistema software (si escludono quindi esplicitamente tutti i formati proprietari dei software commerciali compresi quelli delle suite Microsoft Office – Word, Excel, Powerpoint, Access) e intelligibili nel tempo;
2. essere ottimizzati nella dimensione, per limitare lo spreco di banda e di spazio disco sul server, eventualmente utilizzando un algoritmo di compressione tra quelli successivamente elencati. Il contenuto dei file compressi deve rispettare tutti i principi qui dettati ed essere codificato nei formati elencati;
3. escludere l'utilizzo di password o altre forme di limitazione dell'accesso ai contenuti, in quanto la visibilità del documento deve essere controllata esclusivamente dalle credenziali di accesso in Titulus;
4. escludere la presenza, al loro interno, di codice eseguibile che, in qualunque forma, consenta surrettiziamente modifiche della presentazione o del contenuto dello stesso documento (come ad es. macro, *script*, ecc. e, di conseguenza, virus). Sono ammesse, per i fogli elettronici, le formule e le macro strettamente finalizzate al completamento univoco dei contenuti;
5. avere un nome del tipo *`radice.est`* dove *`radice`* richiami il contenuto o la nomenclatura del documento e l'*`est`*ensione corrisponda convenzionalmente al formato effettivamente utilizzato dal file (ad. es. "`allegato_1.pdf`" per il primo allegato in formato PDF - Acrobat), preferibilmente senza l'utilizzo di spazi, diacritici, punteggiatura e simboli diversi dal trattino "-" e dall'*underscore* "_".

Per quanto sopra esposto gli allegati informatici devono essere in uno dei seguenti formati standard:

- PDF (estensione `.pdf` - Portable Document Format, conosciuto anche come Adobe Acrobat), da preferire per qualsiasi tipologia di documento informatico;

e, nel caso sia necessario consentire al destinatario un agevole rielaborazione delle informazioni ivi contenute, sono ammessi i seguenti formati:

- OpenDocument (estensioni `.odt`, `.ods`, `.odp`, `.odg` - ODF, ISO/IEC 26300, nome completo: OASIS Open Document Format for Office Applications), un formato standard ISO per i documenti elettronici d'ufficio, gestibile mediante la suite libera OpenOffice e anche da Microsoft Office con l'ausilio di appositi moduli aggiuntivi gratuiti (*plugin*), fatto comunque salvo quanto disposto al precedente punto 2.d);
- RTF (estensione `.rtf` - Rich Text Format), formato proprietario di Microsoft per l'interscambio di documenti testuali ma che garantisce, tuttavia, un più esteso supporto da parte di software di terze parti (ivi compresa la suite OpenOffice);
- TXT, testo semplice codificato in ASCII 7 bit ovvero ISO-8859-1 ovvero Unicode UTF-8 o UTF-16 (per il supporto degli alfabeti internazionali);
- Immagini bitmap: JPEG (est. `.jpg` o `.jpeg`), PNG (est. `.png`), TIFF (est. `.tif` o `.tiff`);
- Grafica vettoriale 2D: SVG (est. `.svg` – Scalable Vector Graphic);
- Illustrazioni o modelli tecnici: DXF (est. `.dxf` – Drawing eXchange Format).

Sono ammessi file compressi nei formati Zip, GZip, BZip2 e 7-Zip, non di tipo autoestraente (eseguibili) e rispettare, dove applicabili, i principi elencati nel presente paragrafo.

Al di fuori dei formati specificati l'allegato deve essere registrato previa conversione in PDF o in uno dei formati sopra elencati.

Titolo V - Elenco documenti soggetti a trasmissione in formato analogico cartaceo originale

I documenti per i quali è prevista obbligatoriamente la spedizione in formato analogico cartaceo sono i seguenti:

- fatture
- verbali di laurea
- schede di laurea
- verbali esami di profitto
- verbali di tirocinio
- piani di studio degli studenti
- verbali commissione giudicatrici ammissioni master
- verbali commissioni giudicatrici ammissioni corsi dottorato di ricerca
- verbali commissioni giudicatrici ammissioni corsi di perfezionamento
- verbali commissioni giudicatrici per l'attribuzione dell'assegno per la collaborazione all'attività di ricerca
- verbali sedute di specializzazione
- verbali commissioni giudicatrici per il conferimento del titolo di dottore di ricerca
- verbali commissioni giudicatrici per l'assegnazione di borse di studio post-lauream
- verbali commissioni giudicatrici per l'assegnazione di borse di studio post-dottorato
- verbali commissioni giudicatrici per l'assegnazione di premi di studio
- verbali procedure concorsuali
- libretti delle lezioni dei docenti
- registri delle funzioni didattiche dei docenti
- progetti per i quali è prevista una procedura di sottoscrizione
- originali delle convenzioni per i quali è prevista una procedura di sottoscrizione
- originali atti costitutivi, patti parasociali, statuti relativi ad enti da istituire o cui aderire per i quali è prevista la sottoscrizione dei suddetti atti;
- estratti autentici di deliberazioni e provvedimenti rettorali necessari per la formalizzazione di procedure avviate innanzi a Notai (approvazione atti costitutivi di enti cui intende aderire l'Università; approvazione modifiche di Statuto di enti cui partecipa l'Università; deliberazioni di aumento del capitale sociale di società cui l'Ateneo è socio; etc);
- gli atti richiesti ai fini della produzione in giudizio per le controversie instaurate in danno dell'Università o per quelle in cui l'Ateneo è parte attrice o ricorrente (ivi compresi quelli relativi alla fase preliminare del tentativo obbligatorio di conciliazione ex art. 66 e ss del D. Lgs. 165/2001) e in tutte gli altri procedimenti giurisdizionali comunque promossi;

Il suddetto elenco non è esaustivo ma ha solo valore esemplificativo.
Su richiesta motivata dell'Unità Organizzativa che ne propone istanza devono essere trasmessi, in formato analogico, al richiedente ulteriori documenti.

Disposizioni finali

Per quanto non espressamente previsto si rinvia alla normativa legislativa vigente in materia.

Legenda

«S.I.G.D.»: Sistema Informativo Gestione Documentale
«AOO»: aree organizzative omogenee
«UO»: unità organizzativa
«PEC»: posta elettronica certificata
«RPA»: responsabile di procedimento amministrativo
«RP»: responsabile di procedura amministrativa
«PP.AA.»: pubbliche amministrazioni
«P.A.»: pubblica amministrazione
«CNIPA»: centro nazionale per l'informatica nella pubblica amministrazione
«CAD»: codice dell'amministrazione digitale