UNIVERSITÀ DI PARMA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

SOMMARIO

ELENCO ALLEGATI

Allegato 1	Elenco AOO
Allegato 2	Tipologia di profili
Allegato 3	Tipologie di firma elettronica
Allegato 4	Tipologie di formati
Allegato 5	Utilizzo firma elettronica o firma digitale
Allegato 6	Modello comune di documento informatico
Allegato 7	Metadati
Allegato 8	Repertori attivi
Allegato 9	Titolario di classificazione
Allegato 10	Allegato tecnico per il Servizio di hosting del sistema di gestione documentale.

1 IL MANUALE DI GESTIONE

1.1 CHE COS'È, A COSA SERVE E A CHI SERVE

Il Manuale di gestione è uno strumento operativo concreto che descrive il sistema di gestione dei documenti.

Indica le procedure e fornisce le istruzioni per la corretta trattazione, tenuta e conservazione della documentazione analogica e digitale, descrivendo le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'AOO Dipartimento Di Scienze Economiche E Aziendali secondo parametri di corretta registrazione di protocollo, di assegnazione, classificazione, fascicolazione, reperimento e conservazione dei documenti informatici.

Il manuale di gestione costituisce una guida ed è rivolto a tutto il personale dell'Area Organizzativa Omogenea (AOO) "Dipartimento Di Scienze Economiche E Aziendali".

Esso è redatto sulla base del modello predisposto dal coordinatore della gestione documentale di ateneo.

Gli allegati dettagliati nell'indice possono essere oggetto di autonoma modificazione e/o integrazione in conseguenza di atti o provvedimenti di carattere generale anche organizzativi emanati successivamente all'entrata in vigore del presente manuale.

L'aggiornamento del manuale e/o degli allegati è effettuato a cura del Responsabile della gestione documentale dell'AO dipartimentale.

1.2 FORME DI PUBBLICITÀ E DIVULGAZIONE

Il manuale di gestione è reso pubblico mediante la pubblicazione sul sito dipartimentale.

È capillarmente divulgato al personale del dipartimento al fine di consentire la corretta diffusione delle nozioni e delle procedure di gestione documentale. E' approvato con provvedimento del direttore del dipartimento su proposta del responsabile della gestione documentale.

2 QUADRO ORGANIZZATIVO ISTITUZIONALE

2.1 AREA ORGANIZZATIVA OMOGENEA (AOO) E UNITÀ ORGANIZZATIVA RESPONSABILE (UOR)

L'Area Organizzativa Omogenea (AOO) è un insieme di funzioni e di strutture individuate dall'Ateneo che opera su tematiche omogenee e che presenta esigenze di gestione documentale in modo unitario e coordinato.

L'Unità Organizzativa Responsabile (UOR) è, all'interno della AOO, un complesso di risorse umane e strumentali cui è stata affidata una competenza omogenea, nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari o procedimenti amministrativi.

L'Università degli Studi di Parma è organizzata nelle AOO descritte nell'**ALLEGATO 1**[1]**.**

Ogni struttura dipartimentale costituisce una AOO ed è sull'Indice delle Pubbliche Amministrazioni.

2.2 TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

L'AOO Dipartimento Di Scienze Economiche E Aziendali organizza la funzione di servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali del dipartimento, come previsto dall'art. 61 del DPR n. 445 2000, cui è attribuita la competenza sulla tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.

In particolare essa:

- garantisce la gestione, tenuta e tutela dei documenti nel loro ciclo di vita provvedendo alla normalizzazione degli strumenti e delle procedure;
- assicura la corretta esecuzione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso ai documenti amministrativi e le attività di gestione degli archivi;
- cura la redazione e l'aggiornamento del *Manuale di gestione del protocollo informatico del Dipartimento Di Scienze Economiche E Aziendali* e dei relativi allegati, curandone anche le forme di pubblicità;
- cura la gestione del protocollo informatico e, in dettaglio:
    - garantisce la corretta produzione del registro giornaliero di protocollo;
    - produce il pacchetto di versamento e assicura il trasferimento del suo contenuto al sistema di conservazione secondo le modalità operative definite dal *Manuale di Conservazione*;
    - autorizza le operazioni di annullamento;
    - cura e vigila sul corretto utilizzo della casella di posta elettronica istituzionale e della casella di posta elettronica certificata istituzionale del dipartimento.

[1] Allegato 1: Elenco AOO dell'UniPR

2.3 RESPONSABILE DELLA GESTIONE DOCUMENTALE

In ottemperanza all'art.3 del DPCM 3 dicembre 2013 ogni AOO dell'Ateneo ha un responsabile della gestione documentale. Tale ruolo, nelle strutture dipartimentali, è ricoperto dai RAG.

Il responsabile della gestione documentale assicura la corretta attuazione delle attività di cui all'art.4 DPCM 3 dicembre 2013[2] (Compiti del responsabile della gestione documentale).

Il responsabile della gestione documentale opera d'intesa con il coordinatore della gestione documentale e il responsabile della conservazione.

2.4 PROFILI DI ABILITAZIONI DI ACCESSO INTERNO ED ESTERNO ALLE INFORMAZIONI DOCUMENTALI

Il responsabile della gestione documentale del dipartimento chiede le abilitazioni per ciascun utente al coordinatore della gestione documentale concordando caso per caso le tipologie di abilitazione da attribuire agli utenti del dipartimento. La procedura prevede l'invio di apposito format alla casella supportoprotocollo@unipr.it (si veda l'**ALLEGATO 2**).

2.5 PEC ISTITUZIONALE DELLA AOO

L'Università degli Studi di Parma ha attivato una casella PEC istituzionale per ogni AOO, il cui elenco è pubblicato nel sito dell'IPA e nel sito istituzionale dell'Ente.

L'indirizzo della PEC istituzionale del Dipartimento è: DipScienzeEconomiche@pec.unipr.it

2.6 E-MAIL ISTITUZIONALE

Il Dipartimento Di Scienze Economiche E Aziendali è dotato di una casella istituzionale di posta elettronica per il servizio protocollo protocollodipscienzeea@unipr.it (è compito di chi si occupa del servizio per la gestione del protocollo procedere alla lettura dei messaggi ivi pervenuti almeno una volta al giorno. In relazione alle varie tipologie di email pervenute, saranno adottati opportuni metodi di protocollazione, registrazione, smistamento e conservazione.

Ogni dipendente è dotato di casella istituzionale individuale di posta elettronica.

L'utilizzo della posta elettronica istituzionale è disciplinato dal *Regolamento per l'uso della posta elettronica*.

[2] Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

3 IL DOCUMENTO

3.1 DOCUMENTO: DEFINIZIONE E DISCIPLINA GIURIDICA

Il documento è la "*rappresentazione informatica e non informatica di atti, fatti o dati giuridicamente rilevanti*".

Nell'ambito dell'azione della Pubblica Amministrazione si parla di *documento amministrativo*, inteso come "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*"[3].

Il documento amministrativo può assumere la forma di *documento analogico* e *documento informatico*.

Il documento analogico è la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento informatico è definito come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico è quindi un file digitale ovvero una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata.

A differenza del documento analogico che si caratterizza per la pluralità di forme (scrittura privata, atto pubblico etc.) che sostanziano il diverso valore giuridico probatorio, il documento informatico si caratterizza anche per le tipologie di firme che caratterizzano e diversificano l'efficacia giuridica e probatoria del documento.

La firma elettronica non è, infatti la rappresentazione informatica grafica della firma, ma un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo ad un determinato soggetto.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore giuridico probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. Il documento informatico assume la caratteristica dell'immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale: il tipo di firma utilizzata differenzia il valore giuridico del documento. Si veda a tal proposito l'**ALLEGATO 3[4].**

3.2 REDAZIONE/FORMAZIONE DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al CAD e le regole tecniche di cui all'articolo 71 del CAD.

Il documento informatico, incluso quello amministrativo, è formato mediante una delle seguenti modalità:

a) redazione tramite l'utilizzo di appositi strumenti software.
   Il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica qualificata
   - ✓ o con l'apposizione di una validazione temporale
   - ✓ o con il trasferimento a soggetti terzi con PEC con ricevuta completa

[3] Legge 241/90 cercare articolo

[4] Allegato 2: Tipologia di firma elettronica

- ✓ o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza
- ✓ o con il versamento ad un sistema di conservazione

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico
II tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione.

c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente.
In tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti inter-operanti, secondo una struttura logica predeterminata e memorizzata in forma statica.
In tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Inoltre il documento amministrativo informatico assume le caratteristiche di immodificabilità e integrità con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nei sistemi di gestione informatiche dei documenti.

Il ***documento amministrativo informatico*** *redatti ai sensi della lettera a) dell'elenco sopra riportato, deve contenere la denominazione dell'Ente e l'indicazione di*:

- AOO/ UOR
- Data
- Classificazione
- Indicazioni atte a individuare il fascicolo di competenza
- Numero di allegati, se presenti
- Oggetto
- Destinatario
- Testo
- Sottoscrizione
- Sigla eventuali istruttori

- Elementi che individuano il Responsabile del procedimento amministrativo, ai sensi della legge 241/1990.

L'Amministrazione determina di usare per la formazione (intesa come creazione del documento) e gestione dei documenti informatici le tipologie di formati previste nell'**ALLEGATO 4**.[5]

Il documento va sottoscritto digitalmente prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

L'Amministrazione stabilisce che ***siano dotati di firma digitale tutti coloro che hanno potere di impegnare l'Amministrazione verso l'esterno***.

Le categorie di atti che devono essere sottoscritti con firma digitale sono riportate in ALLEGATO 5[6].

L'Amministrazione stabilisce che i propri documenti siano predisposti su un modello comune di documento informatico, riportato in **ALLEGATO 6**[7].

3.3 REDAZIONE/FORMAZIONE DEL DOCUMENTO AMMINISTRATIVO ANALOGICO

Per *documento analogico* si intende un documento formato utilizzando una grandezza fisica, come, ad esempio le tracce su carta, le immagini contenute nei film e le magnetizzazioni su nastro.

Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto cartaceo prodotto con strumenti analogici (e.g. documento scritto a mano o a macchina da scrivere) o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato su carta). L' originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (e.g. sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

I documenti amministrativi analogici dotati di firma autografa prodotti aventi per destinatario un ente o soggetto terzo, sono di norma redatti in due esemplari, un *originale* per il destinatario e una *minuta* da conservare agli atti del mittente.

Si definisce minuta l'*esemplare del documento conservato agli atti dell'amministrazione pubblica mittente*, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato. Come l'originale va corredata di sigla, firma e sottoscrizione autografe.

Il ***documento amministrativo analogico*** *prodotto deve essere redatto su* ***carta intestata*** *e deve di norma contenere*:

- Indicazione AOO/ UOR
- Data
- Classificazione
- Indicazioni atte a individuare il fascicolo di competenza
- Numero di allegati, se presenti
- Oggetto
- Destinatario
- Testo

[5] Allegato 3: Tipologie di formati dei documenti

[6] Allegato 5: Utilizzo firma elettronica o digitale

[7] Allegato 6: Modello comune di documento

- Sottoscrizione
- Sigla eventuali istruttori
- Elementi che individuano il Responsabile del procedimento amministrativo, ai sensi della legge 241/1990.

Il documento va sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

3.4 IL DOCUMENTO COSTITUITO DAL CORPO DELLA PEC

La posta elettronica certificata (PEC) è un mezzo di trasmissione. Il corpo della email trasmessa/ricevuta tramite PEC costituisce un *documento informatico sottoscritto con firma elettronica semplice* in quanto il mittente, per poter creare ed inviare detta e-mail, deve eseguire un'operazione di identificazione, inserendo il proprio *username* e la propria *password*.

Il corpo delle email trasmesse all'amministrazione universitaria tramite PEC *sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio*.

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento: in tal caso, l'avvenuta consegna del messaggio elettronico consente, tra l'altro, di ricorrere contro terzi.

La PEC, a differenza della posta elettronica semplice, ha le seguenti peculiarità:

- identificazione del mittente, se coincide con l'autore del documento,
- garanzia dell'integrità e della riservatezza dei messaggi,
- data certa di spedizione e consegna dei messaggi,
- ricevuta di avvenuta consegna o avviso di mancato recapito,
- tracciatura dei messaggi a cura del gestore

Nel caso la PEC, inviata o ricevuta, presenti documenti in allegato, e questi rientrino in una delle categorie di atti che devono essere sottoscritti con firma digitale, l'invio tramite PEC non sostituisce la loro firma.

3.5 IL DOCUMENTO COSTITUITO DAL CORPO DELLA E-MAIL ISTITUZIONALE

L'e-mail istituzionale costituisce un *documento informatico sottoscritto con firma elettronica semplice* in quanto il mittente, per poter creare ed inviare detta e-mail, deve eseguire un'operazione di identificazione, inserendo il proprio *username* e la propria *password*.

La e-mail istituzionale può essere costituita da un corpo o da un corpo con allegati.

Le e-mail istituzionale inviate dalla casella istituzionale sono considerate *sottoscritte con firma elettronica semplice* e *sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio*.

Nel caso la email, inviata o ricevuta, presenti documenti in allegato, e questi rientrino in una delle categorie di atti che devono essere sottoscritti con firma digitale, l'invio tramite email non sostituisce la loro firma.

3.6 DISTINZIONE DEI DOCUMENTI IN BASE ALLO STATO DI TRASMISSIONE

I documenti, siano essi analogici che informatici, in base allo stato di trasmissione si distinguono in:

- documenti in *arrivo*

- documenti in *partenza*
- documenti *scambiati tra UOR della stessa AOO* (comunemente detti *documenti interni* o *documenti tra uffici*)
- documenti *scambiati tra AOO dello stesso Ente* (comunemente detti *corrispondenza tra AOO*).

Per ***documenti in arrivo*** si intendono *tutti i documenti di rilevanza giuridico probatoria acquisiti dall'Amministrazione, nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato*.

Per ***documenti in partenza*** si intendono *tutti i documenti di rilevanza giuridico-probatoria prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato*.

Per ***documenti scambiati tra UOR della stessa AOO*** si intendono *tutti i documenti scambiati tra le diverse Unità Organizzative Responsabili (UOR) afferenti alla stessa Area Organizzativa Omogenea (AOO)*. I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Per ***documenti scambiati tra AOO dello stesso Ente*** si intendono *tutti i documenti di preminente carattere giuridico probatorio sottoposti alla protocollazione in partenza per la AOO mittente, e alla protocollazione in arrivo per la AOO ricevente*.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e di norma non sono protocollate.

3.7 DUPLICATO DEL DOCUMENTO INFORMATICO E ANALOGICO

Duplicato informatico

Il duplicato del documento informatico è un documento informatico che, mediante idoneo processo o strumento, assicura che il documento informatico ottenuto sullo stesso sistema di memorizzazione ovvero su un sistema diverso contenga la stessa sequenza binaria del documento informatico di origine. I duplicati informatici *hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche*.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

Duplicato analogico

È *la riproduzione del documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali* (e.g. rilascio del certificato di laurea, della carta di identità etc.

Le firme sul duplicato del documento sono delle autorità preposte al momento in carica.

3.8 COPIA DEL DOCUMENTO INFORMATICO E ANALOGICO: NOZIONE

Dai documenti formati in origine sia su supporto informatico, sia su supporto analogico, possono essere tratte copie, le quali, a loro volta, possono essere fatte su supporto informatico o analogico.

Pertanto, a seconda dei supporti dei documenti possiamo avere le seguenti principali modalità di copia.

Documento originale	Copia/estratto	Tipologia di copia
Analogico	Analogico	1- trascrizione o riproduzione dell'originale che può essere a. copia semplice (la pura trascrizione dell'originale senza riguardo agli elementi formali) b. imitativa (La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia) c. conforme (copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica")
	Informatico	1- copia informatica di documento analogico 2- copia per immagine su supporto informatico di documento analogico
Informatico	Analogico	1- copie su supporto analogico di documento informatico
	Informatico	1- copia informatica di documento informatico

Le copie devono essere effettuate mediante processi e strumenti idonei ad assicurare che le informazioni in esse contenute siano corrispondenti a quelle del documento originale.

Ciò che può cambiare sono la forma e/o il supporto.

Qualora la copia riproduca solo una parte del contenuto del documento, viene definita "*estratto*".

In generale, le copie hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta.

3.9 COPIA ED ESTRATTO INFORMATICI DEL DOCUMENTO AMMINISTRATIVO ANALOGICO

È possibile produrre copia su supporto informatico di documenti amministrativi in origine su supporto analogico. La copia informatica ha il medesimo valore dell'originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge. L'attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica o può essere prodotta come documento separato contenente un riferimento temporale e l'impronta di ogni copia.

In entrambi i casi l'attestazione dev'essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico

separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

Per copia informatica di un documento analogico si intende:

- ✓ copia informatica del documento analogico, data dal documento informatico avente contenuto identico a quello del documento analogico da cui è tratto ma diverso come forma;
- ✓ copia per immagine su supporto informatico di documento analogico, avente contenuto e forma uguali all'originale; si tratta della scansione di un documento analogico oppure di un file (ad esempio un documento in formato *PDF*, *TIFF*, *JPEG, etc.*).

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se ad esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma digitale o altra firma elettronica qualificata:

- ✓ per "*rilascio*" si intende la consegna di un supporto fisico idoneo a ricevere stabilmente la memorizzazione della rappresentazione corrispondente al documento cartaceo e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- ✓ per "*spedizione*" si intende l'inoltro telematico del/dei file corrispondente/i per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica.

Le copie per immagine su supporto informatico di documenti originali formati su supporto analogico hanno la medesima efficacia probatoria degli originali, se:

- ✓ la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'art. 71 del CAD[8];
- ✓ sono formate nel rispetto delle regole tecniche di cui all'art. 71 del CAD e se la loro conformità all'originale non è espressamente disconosciuta.

3.10 COPIA ED ESTRATTO INFORMATICI DI DOCUMENTO AMMINISTRATIVO INFORMATICO

La "*copia informatica di documento informatico*" è un documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico, con diversa sequenza di valori binari. Qualora la copia riproduca solo una parte del contenuto del documento, viene definita "estratto".

Le copie e gli estratti devono essere prodotti in uno dei formati idonei mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.

[8] DECRETO LEGISLATIVO 7 marzo 2005, n. 82 Codice dell'amministrazione digitale - Art. 71 Regole tecniche

La copia o l'estratto così formati, di uno o più documenti informatici, se sottoscritti con firma digitale o firma elettronica qualificata da chi effettua la copia, hanno la stessa efficacia probatoria dell'originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può essere inserita nello stesso documento informatico contenente la copia o l'estratto, oppure prodotta come documento informatico separato; in entrambi i casi l'attestazione dev'essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. Se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

3.11 COPIA ED ESTRATTO ANALOGICI DI DOCUMENTO AMMINISTRATIVO INFORMATICO

Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta.

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 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.

Tranne nei casi in cui il documento rappresenti una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati, l'amministrazione può predisporre le comunicazioni ai suoi utenti come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviare ai propri utenti, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

3.12 METADATI

Con il termine *metadati* si intende l'insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione. Tale insieme è descritto nell'**ALLEGATO 7** del presente manuale, il quale riporta anche le modalità con cui viene assicurato il rispetto dei contenuti minimi.

4 IL FASCICOLO

4.1 IL FASCICOLO: NOZIONE, DEFINIZIONE, FUNZIONE

Il *fascicolo* è l'unità di base dell'archivio. All'interno di ciascun fascicolo i documenti che concorrono ad uno stesso affare e/o procedimento sono inseriti secondo l'ordine temporale di registrazione a protocollo e la loro sedimentazione avviene in modo tale che si individui subito il documento cronologicamente più recente.

Ogni *fascicolo* contiene documenti che concorrono ad una stesso procedimento e sono classificati in maniera omogenea, secondo il grado divisionale attribuito dal titolario di classificazione in base all'oggetto, salvo alcune eccezioni (e.g. fascicolo di personale).

La corretta tenuta del fascicolo garantisce sia la sedimentazione che il diritto di accesso.

Si possono distinguere cinque tipologie di fascicolo:

1. di "*Affare*", conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
2. di "*Attività*", conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;
3. di "*Procedimento amministrativo*", conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale;
4. di "*Persona fisica*", conserva i documenti relativi a diversi procedimenti amministrativi, legati da un vincolo archivistico interno, relativo a una persona fisica (e.g. fascicolo del personale, fascicolo dello studente). La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;
5. di "*Persona giuridica*", conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Il Dipartimento Di Scienze Economiche E Aziendali crea e tratta fascicoli di Affari, Attività e Procedimento Amministrativo

4.2 IL FASCICOLO INFORMATICO: FORMAZIONE, IMPLEMENTAZIONE E GESTIONE

Per ogni procedimento, affare, attività, l'Ateneo ha l'obbligo di conservare in un *fascicolo informatico* gli atti, i documenti e i dati da chiunque siano stati formati. Il *fascicolo informatico* deve recare l'indicazione:

- ✓ dell'AOO;
- ✓ del responsabile del procedimento;
- ✓ dell'oggetto del procedimento;
- ✓ dell'elenco dei documenti contenuti;
- ✓ dell'indice di classificazione (e.g. titolo, classe, sottoclasse, etc.);
- ✓ del numero del fascicolo, che è identificativo di una catena numerica relativamente alla classe di riferimento dell'anno di creazione;
- ✓ della data di apertura e di chiusura del fascicolo.

Il fascicolo può essere ulteriormente suddiviso in sotto-fascicoli e inserti. Queste suddivisioni sono identificate con un'ulteriore catena numerica, gerarchicamente posta al di sotto del numero di fascicolo o del sotto-fascicolo.

L'indicazione dell'Unità Organizzativa Responsabile (UOR) e del Responsabile del Procedimento Amministrativo (RPA) concorrono all'identificazione del fascicolo e al riconoscimento del responsabile. La UOR e l'RPA devono essere gli stessi del documento e del fascicolo.

Ogni qualvolta cambia l'RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento.

4.3 IL FASCICOLO IBRIDO

Il *fascicolo ibrido* è composto da documenti formati su supporto cartaceo (analogico) e su supporto informatico (digitale). Ciò darà origine a due unità di conservazione differenti; l'unitarietà del fascicolo è garantita dal sistema informatico mediante gli elementi identificativi del fascicolo (e.g. anno di creazione, titolo/classe numero del fascicolo) e dal contenuto dei documenti, di cui alcuni sono originali in digitale, mentre altri risultano copie informatiche di documenti cartacei ottenute mediante scansione. Al fine di rendere omogeneo il fascicolo informatico a quello corrispondente analogico evitando la stampa dei documenti informatici, si riportano nel fascicolo analogico gli estremi dei documenti digitali presenti nel fascicolo ibrido.

4.4 RACCOGLITORI

Il *raccoglitore* non è un fascicolo procedimentale, ma un contenitore che raccoglie documenti relativi ad uno stesso affare appartenenti però a procedimenti diversi.

Il raccoglitore non ha una classificazione e una numerazione propria. Ne costituisce un esempio il raccoglitore che contiene tutti i documenti che riguardano un immobile, denominato "fascicolo edilizio".

5 REGISTRI E REPERTORI INFORMATICI

5.1 IL REGISTRO DI PROTOCOLLO

Il *registro di protocollo* istituito presso l'AOO Dipartimento di Scienze Economiche e Aziendali è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento ed è idoneo a produrre effetti giuridici a favore o a danno delle parti. Esso è soggetto alle forme di pubblicità e tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

La numerazione è annuale e parte dal numero *1*; inizia dal 1° gennaio e si conclude il 31 dicembre di ogni anno.

Le attività di registrazione giornaliera, vengono trasmesse entro il giorno lavorativo seguente, al sistema di conservazione, garantendone l'immodificabilità del contenuto. Questo documento, generato in modo automatico dal software di gestione documentale viene denominato *registro giornaliero di protocollo*.

5.2 REPERTORI

Per repertorio si intende il registro in cui vengono annotati con numero progressivo gli atti e i documenti per i quali è prevista la registrazione particolare, individuati in base alla tipologia documentale indipendentemente dalla classificazione archivistica del documento desunta dal piano di classificazione in vigore nell'Ateneo. In **ALLEGATO 8** si riportano i repertori attivi presso l'AOO Dipartimento Di Scienze Economiche E Aziendali.

Tali documenti dovranno comunque essere inseriti nel fascicolo archivistico di loro pertinenza.

Di norma il numero progressivo di repertorio viene affiancato a quello di protocollo.

La numerazione della repertoriazione è annuale e parte dal numero *1*; inizia dal 1° gennaio e si conclude il 31 dicembre di ogni anno. Ogni repertorio dell'AOO Dipartimento Di Scienze Economiche E Aziendali è collegato al registro di protocollo.

5.3 IL REPERTORIO DEI FASCICOLI INFORMATICI

Il *repertorio dei fascicoli informatici* è unico nell'AOO Dipartimento Di Scienze Economiche E Aziendali ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.

Il *repertorio dei fascicoli informatici* è costituito da un elenco ordinato ed aggiornato dei fascicoli istruiti all'interno di ciascuna classe e di ciascun titolo del titolario di classificazione adottato, riportante:

- anno e numero progressivo del fascicolo;
- classificazione nell'ambito del titolario adottato;
- oggetto dell'affare/procedimento/attività;
- UOR responsabile dell'affare/procedimento/attività;
- nominativo del responsabile dell'affare/procedimento/attività;
- date di apertura e chiusura del fascicolo;
- numero dei documenti contenuti nel fascicolo;

- dati relativi alla movimentazione del fascicolo
- stato: chiuso/aperto

6 LA GESTIONE DELL'ARCHIVIO CORRENTE

6.1 NOZIONE

Per archivio corrente si intende il 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 non ancora esaurito. L'archivio corrente potrà essere costituito da fascicoli analogici, informatici e ibridi.

I *fascicoli analogici* (compresa la parte analogica dei fascicoli ibridi) restano collocati presso ogni singola struttura (AOO/UOR) per la parte di propria responsabilità e competenza nel trattamento dell'affare, fino al momento del loro trasferimento nell'archivio di deposito che verrà effettuato a cura del Coordinatore/Responsabile della gestione documentale o un suo vicario.

I *fascicoli informatici* saranno versati in conservazione a cura del Coordinatore/Responsabile della gestione documentale o un suo vicario dopo la loro chiusura.

La consultazione dei fascicoli informatici e ibridi è comunque possibile all'interno del sistema di gestione documentale.

6.2 GLI STRUMENTI DELL'ARCHIVIO CORRENTE

Il trattamento dell'intero sistema documentale dell'Amministrazione pubblica passa attraverso la predisposizione di strumenti di gestione dell'archivio nelle sue diverse fasi. Il *titolario* di classificazione e il *repertorio dei fascicoli* per la fase corrente, ed il *massimario di selezione* della documentazione, nella fase di deposito, sono strumenti basilari per l'organizzazione, l'accesso e la fruizione della documentazione che costituisce l'archivio dell'Ateneo.

6.3 TITOLARIO DI CLASSIFICAZIONE

Il *titolario di classificazione* è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (Titolo/Classe/eventuale sottoclasse) stabilite sulla base delle funzioni e delle attività di competenza dell'Ateneo.

Ciascun documento, *entrata/uscita/tra* uffici, anche non sottoposto a protocollazione, è classificato in ordine alla corrispondenza tra il suo oggetto e la relativa voce attribuibile, desunta dal titolario, e successivamente fascicolato.

La classificazione, necessaria e fondamentale, assegna al documento la collocazione all'interno di un determinato fascicolo. La relazione tra i documenti (vincolo) di un'unità archivistica è garantita dalla classificazione dei documenti che ne fanno parte e da una corretta fascicolazione.

Il titolario di classificazione è corredato da un'appendice denominata *Voci d'indice*. Si tratta di un'ulteriore strumento, strettamente correlato al titolario, che agevola le operazioni di classificazione. In esso sono presenti le possibili varianti, trattate e riportate in modo analitico, che possono essere incontrate nell'oggetto.

Il titolario di classificazione e, di conseguenza, il prontuario delle voci d'indice sono inseriti nel sistema di gestione documentale. Possono essere soggetti a revisione periodica, qualora ciò si renda necessario a

seguito di modifiche di carattere normativo e statutario. In questo caso, essi sono adottati a partire dal 1° gennaio dell'anno successivo a quello di approvazione.

Il sistema di gestione documentale garantisce che le voci del titolario siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della loro produzione. Si riporta in **ALLEGATO 9** il titolario di classificazione dell'Ateneo.

6.4 MASSIMARIO DI SELEZIONE

Il *massimario di selezione* è lo strumento con cui l'Ateneo individua le disposizioni di massima e definisce i criteri e le procedure attraverso i quali la documentazione, decorsi i termini di validità giuridico-probatoria e non rivestendo interesse storico ai fini della conservazione permanente, può essere eliminata, previa autorizzazione dell'organo vigilante.

Le operazioni di selezione e scarto, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'Ateneo, avvengono nella fase di deposito, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione permanente.

Accanto al massimario il *prontuario di scarto* è lo strumento nel quale sono menzionati i tempi di conservazione in relazione alle tipologie documentarie. Le *proposte di scarto* vanno fatte secondo le modalità previste nel manuale di gestione del protocollo dell'Amministrazione Centrale (cap.6 La gestione dell'archivio corrente).

7 PROTOCOLLO INFORMATICO: REGISTRAZIONE E SEGNATURA

Il Registro di Protocollo è un atto pubblico originario che fa fede fino a querela di falso circa la data e l'effettivo ricevimento o spedizione di un documento, di qualsiasi forma e contenuto ed è idoneo a produrre effetti giuridici tra le parti.

Il registro di protocollo ha cadenza annuale, cioè inizia il 1 gennaio e termina il 31 dicembre di ogni anno.

7.1 REGISTRATURA: ELEMENTI OBBLIGATORI IMMODIFICABILI, ELEMENTI OBBLIGATORI MODIFICABILI, ELEMENTI ACCESSORI IMMODIFICABILI, ELEMENTI ACCESSORI MODIFICABILI

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi vanno protocollati.

La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore dal ricevimento; se intercorrono dei giorni festivi nel primo giorno lavorativo utile. Per registrazione di protocollo informatico si intende l'apposizione all'originale del documento in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

Ogni numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo immodificabile. Gli elementi obbligatori del protocollo sono inalterabili ed immodificabili. La registrazione degli elementi obbligatori del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante apposita procedura.

L'inalterabilità e l'immodificabilità della registrazione di protocollo deve essere garantita in via informatica.

La registrazione di protocollo, per ogni documento ricevuto, spedito e trasmesso tra uffici dello stesso ente, è effettuata mediante la memorizzazione di elementi obbligatori immodificabili, elementi obbligatori modificabili, elementi non obbligatori immodificabili ed elementi non obbligatori modificabili.

Elementi obbligatori immodificabili

Gli elementi obbligatori immodificabili servono ad attribuire al documento data, forma e provenienza certa attraverso la registrazione di determinate informazioni rilevanti sul piano giuridico-probatorio. Tali elementi sono obbligatori e resi immodificabili dal sistema informatico.

Essi sono:

1. data di registrazione
2. numero di protocollo
3. corrispondente (mittente per il documento in arrivo; destinatario per il documento in partenza)
4. oggetto
5. impronta del documento informatico
6. numero degli allegati
7. descrizione degli allegati

L'insieme di tali elementi è denominato *«registratura»*.

Elementi obbligatori modificabili

Gli elementi obbligatori modificabili sono:

1. unità organizzativa responsabile del procedimento/affare/attività (UOR)
2. responsabile del procedimento amministrativo (RPA)

3. classificazione archivistica
4. fascicolo

Elementi non obbligatori immodificabili

Gli elementi non obbligatori immodificabili sono:

1. data del documento ricevuto
2. protocollo del documento ricevuto
3. annotazioni

Elementi non obbligatori modificabili

Gli elementi non obbligatori modificabili sono:

1. mezzo di trasmissione del documento
2. durata conservazione
3. note
4. collegamento ad altri documenti o fascicoli

7.2 MODALITÀ DI PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI

Ogni registrazione di protocollo informatico produce un record nella base dati del sistema di gestione documentale. Ogni operazione di inserimento e modifica viene registrata anche su un file di log del sistema di gestione documentale corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione.

Dal sistema di gestione documentale è possibile ottenere l'elenco delle modifiche effettuate su una data registrazione ottenendo in dettaglio:

- operazione effettuata sul documento (inserimento/modifica/visualizzazione/cancellazione);
- operatore che ha effettuato l'operazione
- data e ora in cui l'operazione è stata effettuata
- operatore che ha in carico il documento

permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolazione etc.).

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero viene trasmesso in conservazione entro la giornata lavorativa successiva.

7.3 SEGNATURA

La segnatura di protocollo consiste nell'apposizione o associazione sul documento in originale in forma non modificabile e permanente, delle informazioni registrate sul registro di protocollo. Essa consente di individuare ciascun documento in modo inequivocabile.

Segnatura documento informatico

Le informazioni minime da associare al documento informatico sono:

- il codice identificativo dell'amministrazione;
- il codice identificativo dell'AOO;

- il codice identificativo del registro;
- il numero di protocollo,
- la data di protocollo;
- l'anno solare di riferimento del registro di protocollo.

Oltre alle informazioni minime la segnatura prevede:

- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- il codice identificativo dell'ufficio a cui il documento è assegnato;
- ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

Segnatura documento analogico

Le informazioni da associare al documento analogico, tramite timbro, dovranno contenere le informazioni seguenti, desunte dal sistema di protocollo e gestione documentale:

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;
- il numero progressivo di protocollo
- la data di protocollo nel formato GG/MM/AAAA
- la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento
- l'RPA a cui è assegnato per competenza e responsabilità.

7.4 LA RICEVUTA DI AVVENUTA REGISTRAZIONE

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del protocollista rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico.

La ricevuta di avvenuta protocollazione, prodotta dal sistema di protocollo, deve riportare i seguenti dati:

1. il numero e la data di protocollo
2. l'indicazione dell'AOO che ha acquisito il documento
3. il mittente
4. l'oggetto
5. numero e descrizione degli allegati se presenti
6. l'indicazione di Responsabilità: RPA cui è assegnato il documento per competenza
7. l'operatore di protocollo che ha effettuato la registrazione

Per il documento pervenuto tramite pec la ricevuta di protocollazione è rilasciata direttamente dal protocollo informatico.

Per il documento arrivato tramite mail, se richiesta sarà generata in formato PDF e inviata via mail al mittente.

7.5 MODALITÀ DI REGISTRAZIONI: INFORMAZIONI ANNULLATE O MODIFICATE

Si può ricorrere all'annullamento di una registrazione di protocollo quando anche una sola delle informazioni inserite, generate o assegnate automaticamente dal sistema e registrate in forma immodificabile, è errata.

Il provvedimento di annullamento o l'autorizzazione all'annullamento di una registrazione di protocollo è a cura del responsabile della gestione documentale.

L'annullamento è effettuato solo previa verifica della motivazione indicata e nel caso di documenti in uscita o interni solo se non ancora spediti. Nel caso di documenti in uscita già spediti, si dovrà rettificare con altra registrazione di protocollo.

È possibile l'annullamento di documenti in arrivo per sanare errori di registrazione.

Il documento analogico annullato riporta gli estremi dell'annullamento e viene conservato nel fascicolo analogico.

Il documento informatico annullato riporta gli estremi dell'annullamento e viene conservato nel fascicolo informatico.

Se il documento analogico o informatico costituiscono una tipologia documentale soggetta a registrazione particolare per la quale è prevista la conservazione perenne, lo stesso sarà conservato nel proprio repertorio con la dicitura "annullato"

Esempi per i quali è richiesto l'annullamento possono essere:

1. errore di inserimento anche di uno solo dei dati immodificabili (caso più frequente);
2. il documento registrato deve essere modificato per rettifica del destinatario, del testo o altro;
3. la motivazione per cui il documento è stato prodotto è venuta meno.

7.6 REGISTRAZIONE DIFFERITA

La registrazione differita di protocollo informatico è possibile solo per la tipologia di *"documento in arrivo"*.

Per *"protocollo differito"* si intende la registrazione di documento in arrivo che indica nello specifico la data alla quale si differisce il ricevimento del documento stesso e la causa che ne ha determinato il differimento.

È possibile effettuare la registrazione differita di protocollo, qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi.

7.7 DOCUMENTI ESCLUSI DA REGISTRAZIONE

Documenti esclusi per legge[9] da registrazione:

- gazzette ufficiali
- bollettini ufficiali PA
- notiziari PA
- note di ricezione circolari

[9] DPR 28 dicembre 2000, n. 445 "Disposizioni legislative in materia di documentazione amministrativa. (Testo A)" – Art. 53 Registrazione di protocollo

- note di ricezione altre disposizioni
- materiali statistici
- atti preparatori interni
- giornali
- riviste
- libri
- materiali pubblicitari
- inviti a manifestazioni

Sono parimenti esclusi da registrazione di protocollo:

- certificati medici dipendenti – se pervenuti via PEC vengono registrati ma non protocollati

Documenti esclusi su disposizione dell'Ateneo

- richieste ferie
- richieste permessi retribuiti
- comunicazioni da parte di enti diversi di bandi di concorso
- coordinate bancarie
- estratti conto
- richieste di informazioni
- richieste di certificati

7.8 REGISTRO DI EMERGENZA

Il Responsabile della Gestione documentale, previa intesa con il coordinatore della gestione documentale e con il referente informatico, attiva il registro di emergenza, ogniqualvolta, per cause tecniche, non sia possibile utilizzare la normale procedura informatica.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile della gestione documentale, sentito il coordinatore della gestione documentale, autorizza l'uso del registro di emergenza per periodi successivi.

Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione.

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

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema.

Durante la fase di ripristino, a ciascun documento protocollato nel registro di emergenza, viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in 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 ordinario.

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 registro di emergenza si rinnova ogni anno solare, pertanto, inizia il 1 gennaio e termina il 31 dicembre di ogni anno.

Al termine dell'emergenza si chiude il registro e occorrerà:

1. inserire le registrazioni di emergenza nel protocollo informatico attivando l'apposita funzione;
2. dare comunicazione alla/e struttura/e organizzativa/e dell'amministrazione della revoca dell'emergenza;
3. conservare il registro di emergenza.

8 FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il Dipartimento ha individuato, fra il Personale tecnico amministrativo, alcuni Operatori preposti alla gestione del flusso di lavoro in entrata e in uscita all'interno del Dipartimento.

8.1 DOCUMENTI IN ARRIVO

Colui che effettua le registrazioni di protocollo in entrata registra in modo avalutativo tutti i documenti che possono avere valore giuridico-probatorio.

La documentazione da protocollare viene registrata, classificata e smistata, salvo casi particolari al RAG del dipartimento. L'informativa della registrazione è resa immediatamente disponibile in due modalità:

1. attraverso un messaggio e-mail che il sistema di gestione documentale invia automaticamente alla casella di posta elettronica dell'RPA
2. attraverso l'accumulo nella *"vaschetta"* del menu principale del sistema di gestione documentale

Ricezione documenti su supporto informatico

La corrispondenza su supporto informatico in arrivo perviene secondo le seguenti modalità:

1. documento ricevuto via e-mail istituzionale didattica.sea@unipr.it e amministrazione.sea@unipr.it
   Il documento che perviene alla e-mail istituzionale del Dipartimento e che si ritiene di dovere acquisire a protocollo viene protocollato e smistato.
   I documenti che pervengono su indirizzi mail diversi da quello del protocollo che si ritiene di dovere protocollare *devono essere reindirizzati alla casella del protocollo dipartimentale*.
   Le comunicazioni informali ricevute per posta elettronica che consistano in semplice scambio di informazioni che non impegnino il dipartimento verso terzi non devono essere protocollate.
   I documenti inviati tramite e-mail da privati cittadini o altri soggetti privati possono essere protocollati se sottoscritti con firma digitale, ovvero quando chi invia il documento è identificato tramite il sistema pubblico di identità digitale (SPID) o quando sono sottoscritte e presentate unitamente alla copia del documento di identità.(art.65 dlgs 179/2016)
   All'infuori delle predette ipotesi i documenti pervenuti possono comunque essere registrati nel sistema di protocollo e così acquisiti e fascicolati dall'RPA come documenti non protocollati.
   Le comunicazioni e i documenti ricevuti da altre pubbliche amministrazioni attraverso l'utilizzo della posta elettronica, sono valide se sottoscritte con firma digitale oppure sono dotati di segnatura di protocollo oppure sono trasmessi attraverso sistemi di posta elettronica certificata oppure sono trasmessi tramite sistemi di posta elettronica istituzionale.

2. documento ricevuto via PEC istituzionale DipScienzeEconomiche@pec.unipr.it
   Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale.
   Indipendentemente dal mezzo di trasmissione, è data priorità nella registrazione a protocollo a qualsiasi documento che implica scadenze a breve.

3. Documenti informatici su supporti rimovibili

I documenti digitali possono pervenire anche per vie diverse dalla posta elettronica e supporti diversi: cd, usb, etc. Il documento informatico contenuto nel supporto informatico, solo se leggibile, è acquisito e protocollato. Sarà cura del RPA verificarne le caratteristiche tecnologiche e la provenienza certa.

Ricezione documenti su supporto analogico

La corrispondenza su supporto analogico in arrivo perviene a diversi operatori dipartimentali secondo le seguenti modalità:

1. posta pervenuta per il tramite del Servizio di posta ordinaria;
2. posta pervenuta tramite personale operante nel Dipartimento

Tutte le buste vanno aperte dal personale operante nel Dipartimento Fanno eccezione, e pertanto non vengono aperte, le buste riportanti le seguenti diciture:

1. riservato, personale, confidenziale, spm, o dalla cui confezione si evinca il carattere di corrispondenza privata
2. "offerta", "gara d'appalto" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad esempio ceralacca, etc.).

Ogni dipendente che ricevesse, tramite corrispondenza privata, documenti concernenti affari o procedimenti amministrativi dell'amministrazione è tenuto a farli pervenire tempestivamente alla mail istituzionale del Dipartimento.

Le buste pervenute tramite posta raccomandata, celere e corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione, sono pinzate assieme al documento e con esso fascicolate.

Registratura e segnatura documenti analogici

La registratura e la segnatura dei documenti analogici in arrivo è effettuata dal personale, afferente al Dipartimento, preposto all'utilizzo del Protocollo

Registratura documenti pervenuti via e-mail istituzionale

La registrazione dei documenti arrivati all'indirizzo email protocollodipscienzeea@unipr.it viene effettuata dal personale, afferente al Dipartimento, preposto all'utilizzo del Protocollo.

Registratura documenti pervenuti via pec

I documenti pervenuti via PEC vanno protocollati nella stessa giornata della loro ricezione o, al massimo, nel primo giorno successivo lavorativo utile, qualora siano ricevuti dopo l'orario di chiusura del servizio, in giorni festivi o non lavorativi.

I messaggi di PEC con testo scritto ricevuti privi di documenti informatici in allegato sono da considerarsi come documenti informatici e, pertanto, devono essere protocollati.

Qualora la PEC riceva un documento informatico (sottoscritto con un tipo di firma elettronica) o un documento in copia (ad es., un pdf con il valore stabilito dall'art. 2712 del codice civile), e qualora il messaggio di PEC non contenga informazioni rilevanti (alla stregua di una copertina di trasmissione del telefax), si provvederà alla registrazione di protocollo del documento allegato (e non del messaggio di PEC), menzionando nel registro di protocollo il canale di ricezione o di trasmissione.

Assegnazione

Chi protocolla assegna il documento come RPA al RAG dipartimentale tranne i casi in cui il RAG individui come RPA altra persona all'interno del Dipartimento.

Qualora il documento contenga informazioni di interesse di altre persone l'operatore di protocollo smista ad esse il documento in copia conoscenza (cc).

8.2 PROTOCOLLO RISERVATO

Se il documento, comunque pervenuto, contiene dati sensibili confidenziali o informazioni che il responsabile della gestione documentale ritiene debbano avere una visibilità limitata, verrà registrato nella modalità "riservato" stabilendo per convenzione, come termine di riservatezza, il 31 dicembre del 70° anno successivo alla data di registrazione[10]. L'abilitazione alla visione e gestione dei documenti riservati è prerogativa del direttore di dipartimento e del rag.

8.3 DOCUMENTO IN PARTENZA

I documenti amministrativi vengono formati in modalità informatica o analogica secondo quanto descritto nei par. 3.2 Redazione/formazione del documento amministrativo informatico e 3.3 Redazione/formazione del documento amministrativo analogico, quindi firmati e successivamente protocollati secondo quanto descritto nel cap. 7 Protocollo informatico: registrazione e segnatura.

Per l'invio dei documenti amministrativi informatici, in quanto originali informatici ovvero copie informatiche di documenti analogici, l'Ateneo si avvale dei canali digitali, preferibilmente secondo le seguenti modalità:

1. per i cittadini/persone fisiche, invio all'indirizzo PEC o email da questi dichiarato, ovvero al domicilio digitale eventualmente presente nell'Anagrafe Nazionale della Popolazione Residente (ANPR) in fase di attivazione;
2. per le imprese e i professionisti all'indirizzo email o PEC da essi dichiarato ovvero a quello pubblicato nell'Indice Nazionale degli indirizzi PEC di imprese e professionisti (INI-PEC – www.inipec.gov.it);
3. per gli altri atenei o pubbliche amministrazioni all'indirizzo email o PEC da queste dichiarato ovvero a quello pubblicato nel sito www.indicepa.gov.it.

L'invio tramite email o PEC dei documenti amministrativi originali informatici viene fatto direttamente dal software di protocollo informatico Titulus mediante le apposite funzionalità.

Ai messaggi trasmessi con questa modalità viene automaticamente allegato un file, denominato segnatura.xml, che contiene i metadati del documento.

Per l'invio dei documenti analogici o delle copie analogiche di documenti digitali, il RPA si avvale dei tradizionali sistemi: posta prioritaria, Raccomandata AR, fax, ecc.

8.4 FLUSSO DEL DOCUMENTO INFORMATICO TRA UOR

Il documento tra uffici (o interno) è quello che una UOR invia ad un'altra UOR della stessa AOO.

[10] Decreto legislativo 30 giugno 2003, n. 196

La differenza sostanziale tra documento in partenza e documento scambiato tra uffici sta nel fatto che nel secondo caso due UOR gestiscono lo stesso documento per due attività diverse.

Trattandosi di documenti endoprocedimentali, possono essere prodotti nella sola modalità informatica e la registrazione a protocollo costituisce firma elettronica.

Il firmatario è colui che accede con le proprie credenziali personali al software di protocollo e compie l'operazione. Essendo il dipartimento attualmente organizzato in un'unica UOR per ora non utilizza il protocollo tra uffici.

8.5 FLUSSO DEL DOCUMENTO TRA AOO DELLO STESSO ENTE

Il flusso dei documenti informatici tra AOO dello stesso Ente prevede la registrazione del protocollo in partenza per la AOO mittente e la protocollazione in arrivo per la AOO destinataria.

L'interoperabilità è garantita mediante la cd. "Corrispondenza tra AOO".

Il documento informatico perviene all'AOO di destinazione nella casella "bozze o corrispondenza tra AOO".

9 CASISTICA E COMPORTAMENTI

Nel seguito vengono fornite alcune indicazioni pratiche riguardo ai comportamenti organizzativi da adottare di fronte ad alcune situazioni che possono verificarsi in sede di registratura.

Gli atti giudiziari o i documenti contenenti termini devono essere protocollati prioritariamente agli altri.

9.1 GESTIONE DI GARE DI APPALTO

Le buste riportanti le seguenti diciture: "*offerta*", "*gara d'appalto*" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad es. ceralacca) *non vanno aperte*. La segnatura di protocollo va apposta sulla busta di cui si effettua la scansione ove il formato lo consenta.

Per le offerte consegnate nel giorno di scadenza, sulla busta viene indicata l'ora di consegna, oltre alla segnatura di protocollo.

Se la registrazione avviene dopo l'ora fissata per la consegna o se la consegna avviene dopo la scadenza fissata dal bando di gara, a protocollo viene inserita anche una "*Nota/Annotazione*" in modo immodificabile in cui si dà contezza del fatto, del tipo: "*documento pervenuto/consegnato alle ore HH.MM del giorno GG/MM/AAAA come risulta dall'indicazione riportata sulla busta che si digitalizza*".

9.2 DOCUMENTI DEI MERCATI ELETTRONICI

I mercati elettronici della P.A. sono dei mercati digitali in cui le amministrazioni abilitate possono acquisire, per valori inferiori alla soglia comunitaria, i beni e i servizi offerti da fornitori abilitati.

Il Mercato Elettronico della P.A. (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, è uno strumento di e-Procurement, avviato e gestito da Consip dal 2003, per conto del Ministero di Economia e Finanza, mediante il quale le Pubbliche Amministrazioni possono acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, il cui importo deve essere inferiore alla soglia comunitaria.

Inoltre, l'Agenzia Intercent-ER per lo sviluppo dei mercati telematici della Regione Emilia-Romagna, istituita con Legge Regionale 11 del 2004 ha avviato un suo sistema telematico di negoziazione (e-Procurement), rivolto agli enti della Pubblica Amministrazione aventi sede nel territorio regionale.

All'interno del Mepa/Intercent-ER, quindi, le P.A. dell'Emilia Romagna hanno la possibilità di consultare e confrontare on line un'ampia gamma di proposte offerte dai diversi fornitori abilitati, aderire a una Convenzione o un Accordo Quadro, scegliendo quella più rispondente alle proprie esigenze.

Si utilizzano le seguenti principali procedure di acquisto:

Ordini diretti → Mercato Elettronico

Ordini diretti → Convenzioni

Negoziazioni → Mercato Elettronico

Ordini diretti sulla piattaforma MePA/Intercent-ER

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un ordine diretto, che consiste nel selezionare l'articolo di proprio interesse fra quelli presenti nel catalogo dei fornitori e di effettuare l'ordine di acquisto al fornitore che è in grado di fornire l'articolo al prezzo più conveniente per l'amministrazione.

Il processo può essere così brevemente schematizzato: il punto istruttore effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante. Il punto ordinante, cioè la persona che dispone di potere di spesa e del dispositivo di firma digitale, controlla la bozza, genera attraverso la piattaforma il file pdf che costituisce il documento d'ordine, lo scarica sul proprio PC, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema.

La piattaforma MePA/Intercent-ER chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione.

Ordini Diretti - Convenzioni

Quando l'articolo che si intende acquistare è presente in una delle convenzioni Consip/Intercent-ER attive, l'Amministrazione aderisce a tale convenzione ed effettua un ordine diretto al fornitore che è vincitore della gara precedentemente espletata dalla Consip/Intercent-ER.

Il processo può essere così brevemente schematizzato:

il punto istruttore seleziona la convenzione, effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante.

Il Punto Ordinante controlla la bozza, genera attraverso la piattaforma il file .pdf che costituisce il documento d'ordine, lo scarica sul proprio pc, lo firma digitalmente lo registra nel sistema di protocollo e lo ricarica a sistema. La piattaforma MePA/Intercent-ER chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione.

Negoziazioni (Richieste di Offerta – RdO)

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad una Richiesta di offerta (RdO), che consiste nell'espletamento di una gara telematica con gli strumenti offerti dalla piattaforma Acquistinretepa.it/Intecent-ER.

Nell'esecuzione dell'iter che conduce alla creazione della RdO, è possibile allegare dei documenti prodotti dall'amministrazione, sia di carattere amministrativo che tecnico-economico, al fine di supportare i fornitori nella predisposizione dell'offerta. Esempi di tali documenti sono il disciplinare di gara, il capitolato tecnico, ecc. I documenti che vengono allegati in questa fase sono di norma firmati dal responsabile e preventivamente registrati a protocollo.

Le buste arrivate sulla piattaforma MePA/Intercent-ER si possono aprire solo alla scadenza della gara telematica con una seduta pubblica web. Una volta individuato il soggetto aggiudicatario, il sistema genera automaticamente il documento di stipula che viene firmato digitalmente, registrato nel sistema di protocollo e ricaricato a sistema.

La piattaforma MePA/Intercent-ER chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione.

9.3 GESTIONE DI CONCORSI E SELEZIONI

Poiché le istanze di partecipazione a concorsi, selezioni, etc., sono spesso corredate di allegati numerosi e, in alcuni casi, anche voluminosi, le domande pervenute su supporto cartaceo sono protocollate effettuando la scansione solo della domanda di partecipazione non degli allegati. Di essi viene riportata il numero e la descrizione.

La documentazione per la partecipazione a concorsi, selezioni, etc., per cui non sia stato possibile procedere alla registrazione a protocollo nella giornata di ricezione, deve essere protocollata con provvedimento di differimento della registrazione alla data di ricezione.

Se la documentazione per la partecipazione a concorsi, selezioni, etc., è trasmessa in modalità elettronica a mezzo di posta elettronica certificata viene protocollata e non occorre effettuare nessuna verifica o descrizione degli allegati.

9.4 GESTIONE ATTI GIUDIZIARI

Ai fini dell'identificazione del mittente (corrispondente) di atti e/o note inerenti ad attività contenziosa, occorre tener presente la differenza tra la notifica (effettuata direttamente all'Amministrazione) e altri tipi di comunicazione.

La notifica è effettuata dall'ufficiale giudiziario, tramite il servizio postale o a mezzo PEC.

Per mittente si intende la parte istante, ovvero l'avvocato che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto. Anche un sindacato può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una causa sindacale.

Il mittente del documento non è chi ha notificato l'atto (es. Tribunale, Corte di Appello), ma colui a cui è conferito il mandato (cioè il corrispondente apposto sulla prima pagina dell'atto).

Quando l'atto invece è notificato presso l'Avvocatura Distrettuale o Generale dello Stato, in quanto soggetto che assicura la difesa in giudizio dell'Amministrazione, l'Avvocatura stessa generalmente procede alla trasmissione dell'atto all'Amministrazione, dandone informativa. In tal caso si tratta di una comunicazione, il cui mittente è appunto l'Avvocatura, come per tutte le comunicazioni dalla stessa provenienti.

Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla cancelleria dell'autorità giudiziaria (Tribunale, Corte di appello, etc.) innanzi a cui pende il giudizio. In questi casi il mittente è l'autorità giudiziaria medesima.

9.5 GESTIONE PEC

Ad ogni messaggio ricevuto o spedito da una AOO corrisponde un'unica operazione di registrazione di protocollo. Pertanto, se con un unico messaggio di PEC pervengono due o più istanze il protocollo sarà uno solo.

Qualora la documentazione pervenuta dovesse essere assegnata anche ad AOO diverse appartenenti allo stesso ente, si procede alla registrazione assegnandola alla AOO ricevente e inviando la documentazione tramite posta elettronica, o altro mezzo di spedizione idoneo, anche alle altre AOO destinatarie. I riferimenti di tale invio alle altre AOO (data, mezzo di trasmissione, indirizzo e-mail del destinatario, etc.) dovranno essere riportati nel campo "Annotazione" in modo immodificabile.

Tale procedura di reinoltro dovrà essere seguita anche nel caso dovessero pervenire documenti non destinati alla AOO ricevente, ma ad altra AOO dell'Ateneo. L'AOO ricevente gestirà i documenti ricevuti come "*documento non protocollato*" assegnandoli alla UOR responsabile del protocollo che, a sua volta, inoltrerà il contenuto tramite PEC all'AOO responsabile e procederà alla fascicolazione del documento non protocollato in apposito fascicolo al Titolo dedicato a protocollo e archivio.

La PEC è solo un vettore per la consegna di documenti. Pertanto il mittente è da individuare nel firmatario del documento, che può essere una persona fisica o giuridica.

Nel caso di Pubbliche Amministrazioni, per una corretta individuazione è necessario ricercare l'AOO mittente, in primo luogo partendo dagli elementi presenti nella segnatura di protocollo del mittente. Qualora permangano dubbi o nella segnatura di protocollo non sia presente l'informazione relativa all'AOO, si procederà ad effettuare la ricerca nell'Indice delle Pubbliche Amministrazioni (IPA). Qualora il documento inviato sia firmato in modo generico (es.: "la Segreteria"), ma dalla tipologia di indirizzo di PEC si desume che si tratta di una Pubblica Amministrazione, si provvede a farne ricerca nell'indice delle PA.

Nel caso una persona fisica utilizzi come vettore l'indirizzo di PEC di altra persona giuridica/fisica, il mittente sarà il firmatario del documento e si effettuerà la relativa annotazione nella registrazione di protocollo.

Per i professionisti che utilizzano un indirizzo di PEC individuale per l'invio di documenti nell'ambito della propria attività, si procederà a creare un'anagrafica di persona giuridica intestata alla società come rinvenibile dalla documentazione (es: Studio Legale Rossi Mario e soci), associandovi l'indirizzo individuale.

Nei casi in cui però utilizzano il proprio indirizzo di PEC per l'invio di documenti non inerenti l'attività professionale, il mittente è la persona (fisica o giuridica) che si ricava dall'analisi del documento trasmesso.

Per i professionisti che svolgono attività di curatela fallimentare su incarico di Tribunali (avvocati, commercialisti, etc.) si crea un'anagrafica di persona giuridica, indicando l'indirizzo di PEC per la specifica curatela nell'area apposita.

Qualora il documento sia riconducibile ad un'attività svolta in collaborazione da più entità (pubbliche e/o private) e non sia individuabile il mittente in maniera univoca (promotore principale), si indica come corrispondente il primo di essi, come desumibile dalla sottoscrizione o dalla carta intestata, e si indica nel campo "Note/Annotazione" in modo immodificabile gli altri possibili co-mittenti.

Se nonostante la ricerca in IPA o in altri portali ufficiali non si individua il mittente, si riporta nel relativo campo l'indirizzo di PEC di provenienza. Questo perché, qualora il documento pervenuto generasse procedure di rilevanza giudiziaria, si certifica "fino a querela di falso" l'inviante che potrà essere individuato mediante controlli presso l'ente gestore del servizio di PEC dagli organi competenti.

9.6 IL SECONDO ESEMPLARE DEL DOCUMENTO ANALOGICO/INFORMATICO

Per essere certi che si tratti di un secondo originale di un documento già protocollato è necessario verificare l'esatta corrispondenza tra i due esemplari, inclusi gli allegati, in tutte le loro parti (firme, date, etc.). Per i documenti sottoscritti con firma elettronica è necessario verificare anche che la data di firma coincida.

Una volta appurata la perfetta identità tra i due documenti, si agirà diversamente nel trattamento a seconda della modalità di ricezione del secondo esemplare.

Se il secondo esemplare perviene in formato analogico, si appone su di esso la segnatura di protocollo e l'indicazione "Secondo esemplare". Nella registrazione di protocollo si inserisce la "Nota/Annotazione" in modo immodificabile del tipo "Pervenuto secondo esemplare mediante RR/Posta/Mano" al fine di poter recuperare tutti gli esemplari pervenuti nel caso si debba, ad esempio, modificare la UOR indicata nella segnatura di protocollo.

Nel caso di arrivo mediante PEC o altro sistema informatico (e-mail semplice, etc.) si effettua una registrazione come "*Documento non protocollato*", riportandovi tutti i dati già inseriti nella registrazione di protocollo del primo esemplare (oggetto, mittente, RPA, classificazione, fascicolo, etc.). Si inserisce, inoltre,

la “Nota/Annotazione” in modo immodificabile del tipo “*Il documento non è stato protocollato in quanto trattasi di secondo esemplare del documento già pervenuto e registrato col prot. n. 000000 del GG/MM/AAAA*”.

9.7 DOCUMENTAZIONE CONTABILE: FATTURA ELETTRONICA

A far data dal 31 marzo 2015 è obbligatorio emettere fatture elettroniche nei confronti di tutte le pubbliche amministrazioni, sia per il ciclo attivo che per quello passivo. La fattura elettronica ai sensi dell’articolo 21, comma 1, del DPR 633/72 è la sola tipologia di fattura accettata dalle Amministrazioni, il cui contenuto è rappresentato in un file XML (eXtensible Markup Language). L’autenticità dell’origine e l’integrità del contenuto sono garantite dall’apposizione della firma elettronica qualificata di chi emette la fattura e la trasmissione è vincolata alla presenza del codice identificativo univoco dell’ufficio destinatario della fattura riportato nell’Indice delle Pubbliche Amministrazioni e al Sistema di Interscambio che funge da collettore per tutte le fatture elettroniche di tutte le Pubbliche Amministrazioni.

Non si accettano più fatture cartacee emesse in data pari o successiva al 31 marzo 2015, salvo per i soggetti non tenuti a rispettare l’obbligo di fatturazione elettronica (es. fornitori esteri, persone fisiche o giuridiche senza partita IVA). In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata, registrata nel registro delle fatture e fascicolata.

La fattura elettronica pervenuta nella modalità corretta viene protocollata mediante sistema automatizzato e contestualmente assegnata all’ufficio contabile competente per la registrazione della stessa sul registro delle fatture, entro 10 giorni dal ricevimento della stessa (DL 66/2014 art. 42).

La data di protocollo fa fede quale termine iniziale dei 15 giorni entro cui la fattura va accettata o rifiutata con motivazione (la mancata notifica di rifiuto entro 15 giorni equivale ad accettazione), nonché dei 30 giorni previsti dalla legge decorsi i quali, in assenza di pagamento, iniziano automaticamente a decorrere gli interessi moratori (Dlgs 192/2012, art. 1 comma 1 lett d).

Le fatture elettroniche che saranno trasmesse dai fornitori alle PA dovranno essere obbligatoriamente conservate in modalità elettronica, secondo quanto espressamente disposto dalla legge.

9.8 DURC

Ai sensi dell’art. 4 della Legge 78/2014 la verifica della regolarità contributiva avviene con modalità esclusivamente telematiche. La risultanza dell’interrogazione ha validità di 120 giorni dalla data di rilascio e sostituirà ad ogni effetto il Documento unico di regolarità contributiva (DURC), ovunque previsto, fatta eccezione per le ipotesi di esclusione individuate dalla legge.

La verifica della regolarità contributiva è l’attestazione dell’assolvimento, da parte dell’impresa, degli obblighi legislativi e contrattuali nei confronti di INPS, INAIL e Cassa Edile.

Trattandosi di documento necessario alla corretta documentazione in caso di acquisizione di lavori/beni/servizi, il DURC è acquisito come documento non protocollato e inserito nel fascicolo corrispondente a cura della UOR.

Le notifiche di disponibilità dell’esito della verifica della regolarità contributiva generate attualmente dal sistema di INPS/INAIL/CASSA EDILE e trasmesse tramite PEC non sono soggette a protocollazione; è possibile registrare nel sistema di gestione documentale le stesse notifiche come documento non protocollato.

Si registra a protocollo, invece, la notifica di scadenza dei 30 giorni dalla data di richiesta del DURC che annulla il silenzio-assenso o l'annullamento della richiesta in quanto difforme dai casi previsti dall'art. 9, comma 1, del DM 30 gennaio 2015.

9.9 DOCUMENTI ANONIMI - ANALOGICO E DIGITALE

La *ratio* che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntata alla avalutatività. In altre parole, l'operatore di protocollo deve attestare che un determinato documento così come si registra è pervenuto. Si tratta dunque di una delicata competenza di tipo certificativo, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

Le lettere anonime, pertanto, vanno protocollate. Nel campo mittente va indicata l'anagrafica *Anonimo* o *Mittente Anonimo* e viene normalmente assegnata una visibilità riservata.

10 DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO

10.1 ARCHIVIO CORRENTE

La responsabilità della tenuta dell'archivio corrente è del responsabile del procedimento, affare o attività che produrrà il fascicolo o la serie documentaria.

10.2 ARCHIVIO DI DEPOSITO

Il Dipartimento conserva nell'archivio di deposito i documenti di maggiore rilevanza quali ad esempio verbali organi del dipartimento, documenti relativi ad elezioni, verbali dei corsi di studio ecc. Registro di carico e scarico

Il responsabile della gestione documentale del dipartimento tiene traccia delle eventuali richieste di prelevamento dei fascicoli dall'archivio del dipartimento in un apposito registro di scarico e carico nel quale riporta i dati identificativi del fascicolo, il nominativo del richiedente, la motivazione, la data della richiesta, la data di evasione della richiesta, la data della effettiva restituzione ed eventuali note sulla documentazione consegnata.

11 IL SISTEMA INFORMATICO DI GESTIONE DEI DOCUMENTI

Il sistema informatico è l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. (DPR 445/2000, art.1, lettera r).

La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in arrivo, in partenza e interna) dalle amministrazioni. Ogni AOO individua le misure di sicurezza da adottare secondo quanto stabilito dalle normative vigenti.

11.1 IL MODELLO ORGANIZZATIVO

I servizi di information and communication technology per il supporto all'attività amministrativa e per le esigenze della didattica e della ricerca dell'Ateneo sono curati dall'Area Sistemi Informativi.

Nell'ambito della gestione documentale, l'Ateneo ha acquisito - secondo il modello in house providing - dal Consorzio Cineca l'applicativo **Titulus** con una soluzione di tipo Software as a Service (SaaS): le funzionalità del programma sono rese disponibili attraverso un sito web, il cui accesso è subordinato a un processo di autenticazione informatica.

La documentazione tecnica ed operativa del software Titulus è accessibile al seguente link: http://wiki.titulus.it/doku.php

La conduzione operativa del sistema è curata direttamente al Consorzio Cineca, a cui, in virtù di un'apposita convenzione, sono demandati gli oneri di installazione, manutenzione, gestione, aggiornamento, monitoraggio di tutte le componenti fisiche e logiche infrastrutturali, di verifica della correttezza delle funzioni applicative e dell'integrità delle basi di dati in conformità a quanto previsto dalla normativa vigente in materia di sicurezza e di protezione dei dati e di continuità operativa.

11.2 SICUREZZA DEL SISTEMA INFORMATICO DI GESTIONE DEI DOCUMENTI

Il presente paragrafo descrive le misure di sicurezza (piano per la sicurezza) previste per il sistema di gestione informatica dei documenti, nel rispetto di quelle descritte nel disciplinare tecnico di cui all'All. B del D.Lgs. 196/03 e successive modificazioni, in coerenza con quanto previsto in materia dagli Artt. 50-bis e 51 del Codice dell'Amministrazione digitale e dalle relative regole tecniche emanate dall'AGID.

Le misure di sicurezza del sistema di gestione informatica dei documenti si applicano a tutto il ciclo di vita, dalla fase di attivazione alla fase di esercizio (immissione, gestione e messa a disposizione dei documenti), alla fase di terminazione del servizio ed alle connesse attività di natura tecnologica, quali analisi, progettazione, sviluppo, manutenzione delle infrastrutture, dei sistemi e delle applicazioni.

L'Ateneo di Parma adotta tutte le misure organizzative, procedurali e tecnologiche utili a garantire i necessari requisiti di sicurezza, ed in particolare:

- riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha diritto e necessità;
- integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne ha diritto e necessità;

- disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne hanno diritto e necessità;
- continuità della disponibilità del servizio per i processi e gli utenti che ne hanno diritto e necessità.

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, parte delle funzioni/responsabilità di sicurezza sono demandate a Cineca e descritte **nell'Allegato 12 – Allegato tecnico per il Servizio di hosting del sistema di gestione documentale**.

All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

Per assicurare che tali requisiti di sicurezza siano correttamente presidiati e garantiti, l'Ateneo ha identificato, applicato e descritto il proprio insieme di misure e controlli validi per il sistema di gestione dei documenti digitali, come descritto nel presente capitolo e nei regolamenti: Politica di sicurezza informatica (in fase di definizione), Regolamento per l'utilizzo e l'erogazione dei servizi e delle risorse informatiche (in fase di definizione), Regolamento per la posta elettronica (in fase di definizione), Regolamento PEC e Regolamento postazione di lavoro (in fase di definizione).

In particolare l'Ateneo si impegna a sostenere il proprio sistema di gestione della sicurezza:

- definendo le misure di sicurezza del sistema di gestione informatica dei documenti, associando specifici controlli di sicurezza atti a limitare il rischio connesso alle attività di gestione dei documenti;
- descrivendo i singoli ambiti di controllo e le attività operative (le procedure attinenti la sicurezza);
- applicando tali misure di sicurezza a tutto il personale interno, i fornitori e le terze parti e gli enti produttori, coinvolto a vario titolo nel processo informatica dei documenti;
- applicando tali misure di sicurezza ad ogni asset che compone il sistema di gestione dei documenti digitali (organizzativo, procedurale, applicativo, infrastrutturale, ecc.);
- definendo ed attribuendo ruoli e responsabilità per i diversi elementi di competenza del Cineca e della AOO, relative alle misure di sicurezza;
- sensibilizzando le parti interessate e coinvolte sulla sicurezza delle informazioni;
- determinando obiettivi specifici per la sicurezza delle informazioni, appropriati per i vari ambiti di attività;
- facilitando il controllo delle misure e dei controlli di sicurezza complessivamente attuati, mediante attività di monitoraggio, verifica e controllo, di gestione e di prevenzione degli incidenti e di continuità operativa, sempre in armonia con le strategie dell'organizzazione;
- impegnandosi nella revisione periodica delle misure di sicurezza;
- facilitando il miglioramento continuo del sistema di gestione della sicurezza, composto da tali misure, recependo modifiche nell'organizzazione o nel contesto e assicurando le risorse sufficienti per gestirlo e mantenerlo.

Al fine di garantire i requisiti di riservatezza, integrità, disponibilità e continuità dei dati e delle informazioni contenute nel sistema informatico di gestione dei documenti, sono definite le seguenti **misure di sicurezza**:

- Autenticazione
- Profilazione
- Registrazione degli accessi ed eventi
- Sicurezza delle reti e dei sistemi
- Sicurezza fisica
- Controlli ambientali
- Politiche di salvataggio dei dati e piano di continuità tecnologica

Autenticazione

L'accesso all'applicazione di gestione documentale è consentito al personale di Ateneo che, per il ruolo o per una specifica funzione, ha necessità di trattare i dati in esso conservati (consultazione, inserimento, gestione utenze, ecc.) in accordo con la **Politica di sicurezza informatica** di ateneo ed il **Regolamento per l'utilizzo e l'erogazione dei servizi e delle risorse informatiche** ed avviene tramite il sistema di autenticazione centralizzata di Ateneo.

Profilazione

La profilazione degli utenti si basa su un sistema di autorizzazione, suddiviso in profili descritti nell'**Allegato 2 – Tipologie di profilo**.

Il Coordinatore della gestione documentale attribuisce il profilo ad ogni utente del sistema di gestione documentale.

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

Queste, in sintesi, sono:

- consultazione, per visualizzare in modo selettivo, le registrazioni di protocollo proprie od eseguite da altri;
- inserimento, per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- modifica, per modificare i dati opzionali di una registrazione di protocollo;
- annullamento, per annullare una registrazione di protocollo autorizzata dal Responsabile del registro di protocollo.

Tale profilazione deve essere concessa in coerenza con il trattamento dei dati personali e sensibili (normativa privacy).

Il sistema di gestione del protocollo informatico:

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

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza), in coerenza con la struttura organizzativa della AOO.

Ogni responsabile di protocollo di AOO esegue attività periodiche di monitoraggio, verifica e controllo per accertare che la profilazione del sistema informatico di gestione sia coerente con le mansioni assegnate.

Registrazione degli accessi ed eventi

Il sistema informatico di gestione deve assicurare la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire:

- l'identificazione dell'utente (art. 7, commi 1, lettera d) delle Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale)
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore (art. 7, commi 3 delle Regole tecniche per il protocollo informatico)

Tali registrazioni sono periodicamente salvate con modalità tali da garantirne l'immodificabilità.

In conformità con il provvedimento del Garante Privacy del 28 novembre 2008 sugli amministratori di sistema, il fornitore del servizio assicura quanto richiesto dalla norma.

Sicurezza delle reti e dei sistemi

La rete locale di ateneo è protetta da accessi non autorizzati mediante sistemi di firewalling e regole ACL.

I PC degli utenti sono protetti da sistemi antivirus con aggiornamento quotidiano.

Sugli stessi vengono regolarmente installati (con frequenza almeno semestrale) gli aggiornamenti software volti a prevenirne la vulnerabilità e a correggerne i difetti.

Per quanto riguarda la sicurezza delle reti e dei sistemi del fornitore del servizio, si rimanda al paragrafo 2 dell'**Allegato 12 – Servizio di hosting del sistema di gestione documentale.**

Sicurezza fisica

L'accesso fisico al data center, dove sono contenuti i server dedicati alla componente locale di Ateneo (server di autenticazione centralizzati), è controllato tramite badge. Le autorizzazioni di accesso sono concesse dal responsabile della UOS Erogazione Servizi, che procede periodicamente alla revisione degli accessi.

Per quanto riguarda la sicurezza fisica del fornitore del servizio, si rimanda al paragrafo 2 dell'**Allegato 12 – Servizio di hosting del sistema di gestione documentale**.

Controlli ambientali

Sono previsti appositi controlli ambientali del data center, dove sono contenuti i server dedicati alla componente locale di Ateneo (server di autenticazione centralizzati), quali pavimento galleggiante, impianto di condizionamento, rilevatori di fumo, estintori a CO2, UPS e gruppo elettrogeno.

Sono eseguiti verifiche e test periodici per assicurare che i controlli ambientali funzionino correttamente e siano adeguatamente disegnati ed applicati per le necessità di ateneo.

Per quanto riguarda i controlli ambientali e relative verifiche periodiche del fornitore del servizio, si rimanda al paragrafo 2 dell'**Allegato 12 – Servizio di hosting del sistema di gestione documentale**.

Politiche di salvataggio dei dati e piano di continuità tecnologica

Per la componente locale di Ateneo (server di autenticazione centralizzati), sono state attuate alcune azioni mirate a ridurre il rischio di mancanza del servizio attraverso la ridondanza delle infrastrutture tecnologiche.

L'infrastruttura tecnologica è divisa in tre componenti:

- server CAS-Shibboleth la cui continuità è garantita dal servizio VMware VMotion HA.
- directory server LDAP, la cui continuità è garantita dalla ridondanza del servizio su 3 macchine virtuali;
- server Oracle la cui continuità è garantita dal servizio VMWare VMotion HA .

Sono eseguiti i salvataggi della piattaforma di autenticazione, con periodicità giornaliera sia per le macchine virtuali che per le macchine fisiche con retention di 15 giorni.

Per quanto riguarda le politiche di salvataggio ed il piano di continuità tecnologica del fornitore del servizio, si rimanda ai paragrafi 3 e 5 dell'**Allegato 12 – Servizio di hosting del sistema di gestione documentale**.

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 1

AREA ORGANIZZATIVA OMOGENEA (AOO)

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

ELENCO AREA ORGANIZZATIVA OMOGENEA (AOO)

Si riporta nel seguito l'elenco delle Aree Organizzative Omogenee dell'Università degli Studi di Parma

1) Amministrazione Centrale
2) Dipartimento di Scienze Medico-Veterinarie
3) Dipartimento di Scienze Matematiche, Fisiche ed Informatiche
4) Dipartimento di Giurisprudenza, di Studi Politici e Internazionali
5) Dipartimento di Scienze Chimiche, della Vita e della Sostenibilità Ambientale
6) Dipartimento di Scienze Economiche e Aziendali
7) Dipartimento di Ingegneria e Architettura
8) Dipartimento di Medicina e Chirurgia
9) Dipartimento di Discipline Umanistiche, Sociali e delle Imprese Culturali
10) Dipartimento di Scienze degli Alimenti e del Farmaco
11) Centro di Eccellenza per la Ricerca Tossicologica – CERT
12) Centro di Eccellenza per lo Sviluppo e l'Innovazione Tecnologica – CERIT
13) Centro di Ricerca Interdipartimentale per il Packaging – CIPACK
14) Centro di Ricerche sullo Sport – CeRS
15) Centro di Servizi per la Salute, Igiene e Sicurezza nei Luoghi di lavoro
16) Centro del Sonno
17) Centro Interdipartimentale di Ricerca in Oncologia Molecolare Translazionale – COMT
18) Centro Interdipartimentale di Ricerca in Medicina dello Sport e dell'Esercizio Fisico – SEM
19) Centro Interdipartimentale di Ricerca per l'Innovazione dei prodotti per la salute – BIOPHARMANET-TEC
20) Centro Interdipartimentale di Ricerca FUTURE TECHNOLOGY LAB
21) Centro Interdipartimentale di Ricerca UNIPR – CO LAB
22) Centro Interdipartimentale di Sicurezza Stradale – DISS
23) Centro Interdipartimentale Misure "Giuseppe Casnati"
24) Centro Interdipartimentale per l'Energia e l'Ambiente – CIDEA
25) Centro Interdipartimentale per la Sicurezza, Tecnologie e Innovazione Agroalimentare – SITEIA.PARMA
26) Centro Multidisciplinare Interdipartimentale Lattiero Caseario – MILC
27) Centro per le Attività e le Professioni delle Arti e dello Spettacolo – CAPAS
28) Centro Studi e Archivio della Comunicazione - CSAC
29) Centro Universitario CENTROACQUE.EU
30) Centro Universitario di Odontoiatria
31) Centro Universitario per la Cooperazione Internazionale – CUCI
32) Centro Studi in Affari Europei Internazionali – CSEIA
33) Cento Universitario di Bioetica – UCB
34) Centro Studi Catulliani – CSC
35) Centro di Statistica Robusta per Grandi Banche Dati – Ro.Sta.B.Da.C.
36) Centro Servizi E-Learning e Multimediali di Ateneo
37) OPBA - Organismo Preposto al Benessere degli Animali dell'Università degli Studi di Parma

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 2

TIPOLOGIA DI PROFILI

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1 TIPOLOGIA DI PROFILI

1.1 PROFILI ASSEGNATI

L'elenco aggiornato dei profili assegnati è presente nell'applicazione TITULUS. Per la consultazione dello stesso è necessario rivolgersi all'ufficio Protocollo che coordina la gestione documentale di Ateneo.

1.2 PROFILI A RICHIESTA

- **VISUALIZZATORE**: visualizza i documenti che gli sono assegnati per competenza e conoscenza;
- **OPERATORE**: visualizza e opera sui documenti assegnati e della UOR di appartenenza;
- **DIRIGENTE**: visualizza e opera sui documenti dell'intera area che coordina;
- **SEGRETERIA DI RETTORATO E DIREZIONE**: visualizza tutti i documenti registrati nell'AOO e opera sui documenti della UOR di appartenenza;
- **RESPONSABILE PROTOCOLLO**: visualizza e opera sulla totalità dei documenti registrati;
- **REPONSABILE PROTOCOLLO AOO**: visualizza e opera sui documenti dell'AOO di cui è responsabile;
- **PRORETTORE**: visualizza i documenti assegnati all'area di cui è prorettore;
- **DELEGATO**: visualizza i documenti che gli vengono assegnati in copia conoscenza;

Ogni tipologia di profilo, a seconda delle esigenze legate alla UOR di appartenenza, può essere visualizzatore o operatore dei documenti registrati nei repertori o fascicolati nei fascicoli studente o del personale.

1.3 MODALITÀ PER RICHIEDERE L'ATTIVAZIONE DEI PROFILI

La richiesta per l'attivazione dei profili, dovrà essere inviata tramite indirizzo email istituzionale a *supportoprotocollo@unipr.it* compilando l'apposito format che sarà reso disponibile sulla pagina web del protocollo, il cui template è qui riportato.

FORMAT PER RICHIESTA CREAZIONE E/O MODIFICA PROFILI TITULUS

STRUTTURA DI APPARTENENZA _____

NOMINATIVO _____

MATRICOLA _____

ABILITAZIONE RICHIESTA

- ☐ **VISUALIZZATORE** (visualizza i documenti che gli sono assegnati per competenza e conoscenza)
- ☐ **OPERATORE** (visualizza e opera sui documenti assegnati e della UOR di appartenenza)
- ☐ **DIRIGENTE** (visualizza e opera sui documenti dell'intera area che coordina)
- ☐ **SEGRETERIA DI RETTORATO E DIREZIONE** (visualizza tutti i documenti registrati nell'AOO e opera sui documenti della UOR di appartenenza)
- ☐ **RESPONSABILE PROTOCOLLO** (visualizza e opera sulla totalità dei documenti registrati)
- ☐ **REPONSABILE PROTOCOLLO AOO** (visualizza e opera sui documenti dell'AOO di cui è responsabile)
- ☐ **PRORETTORE** (visualizza i documenti assegnati all'area di cui è prorettore)
- ☐ **DELEGATO** (visualizza i documenti che gli vengono assegnati in copia conoscenza)

EVENTUALE ACCESSO AL FASCICOLO DEL PERSONALE/STUDENTE _____

EVENTUALE TRASFERIMENTO DOCUMENTI/FASCICOLI _____

NUOVO RPA _____

_____

Firma Responsabile

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 3

TIPOLOGIA DI FIRMA ELETTRONICA

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1 TIPOLOGIA DI FIRMA ELETTRONICA

1.1 DEFINIZIONI

Il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (cd Regolamento eIDAS), che si applica dal 2 luglio 2016, definisce le seguenti firme:

1) *firma elettronica*, dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;
2) *firma elettronica avanzata*, una firma elettronica che soddisfi i seguenti requisiti:
   a) è connessa unicamente al firmatario;
   b) è idonea a identificare il firmatario;
   c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
   d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
3) *firma elettronica qualificata*, una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche

Lo stesso Regolamento definisce «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

La *firma digitale* viene definita a livello nazionale dal Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale (CAD):

- *firma digitale*: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

1.2 ESEMPI DI IMPLEMENTAZIONE

Partendo dalle definizioni, per loro natura tecnologicamente neutre, le varie tipologie di firma sono state realizzate in diverse modalità, delle quali vengono forniti alcuni esempi:

1.2.1 Firma elettronica *semplice*

L'esempio più comune di utilizzo di dati elettronici come firma elettronica si ha quando si compiono operazioni o si producono documenti a seguito dell'accesso ad un sistema informatico mediante username e password.

In questo modo, username e password, associati logicamente alle operazioni effettuate o al documento prodotto nel sistema, ne costituiscono la firma elettronica.

Anche un messaggio trasmesso tramite email può essere ritenuto firmato elettronicamente dal mittente, poiché l'accesso al sistema di posta avviene mediante credenziali (di solito username e password) e nel sistema stesso viene mantenuta l'associazione logica fra il messaggio inviato e le credenziali del mittente.

1.2.2 Firma elettronica *avanzata*

Un esempio di firma elettronica avanzata si ha nella firma cosiddetta ***grafometrica,*** che è una modalità di firma elettronica realizzata con un gesto manuale del tutto analogo alla firma autografa su carta. I dati di firma si ottengono mediante un dispositivo elettronico (ad esempio un particolare tablet) in grado di acquisire dinamicamente il movimento di uno stilo - azionato direttamente dalla mano di una persona - su una superficie sensibile (emulando una penna sulla carta).

Essa colleziona dati biometrici del firmatario (e.g. pressione, velocità di firma, tratto, etc.) e li fonde in maniera permanente al documento da sottoscrivere in maniera tale che questi dati biometrici non siano più intellegibili a chi accede al documento.

La firma elettronica avanzata è disciplinata dal DPCM del 22/2/2013: essa può essere usata solamente nei rapporti fra il soggetto che intende avvalersene e i soggetti terzi con cui, per motivi istituzionali, societari o commerciali, intrattiene rapporti.

Per le sue caratteristiche di semplicità (non richiede particolari dispositivi e ricalca il gesto compiuto durante la firma autografa), è molto indicata nei casi in cui si abbia necessità frequente di raccogliere firme da una platea ampia di soggetti, ad esempio negli sportelli al pubblico che erogano servizi (uffici postali, banche, ecc.)

Come verrà descritto in seguito, non è idonea a firmare qualunque tipo di atto, in particolare quelli che trattano di particolari diritti relativi ai beni immobili.

1.2.3 Firma elettronica *qualificata e digitale*

La firma elettronica qualificata e quella digitale, che ne rappresenta un caso particolare, richiedono necessariamente un dispositivo per la loro creazione e un certificato qualificato, cioè un certificato che deve essere rilasciato da un soggetto che ha espletato una apposita procedura di certificazione e che quindi fornisce garanzie maggiori in ordine alla sua affidabilità.

Al momento l'unico modo effettivo di apporre una firma qualificata è tramite la firma digitale, che funziona mediante una doppia chiave crittografica, una pubblica e una privata.

Il dispositivo di firma può essere in possesso del firmatario (es. chiavetta USB, smart card) oppure risiedere presso un soggetto terzo quando si adotta il sistema della cosiddetta firma remota.

Per ragioni di sicurezza, l'apposizione della firma è protetta da PIN, password o da una combinazione di questi.

I file firmati digitalmente possono avere più formati, identificati dalle seguenti estensioni:

- P7M, che identifica lo standard denominato CAdES e consente di firmare digitalmente qualunque tipo di file;
- PDF, che identifica lo standard PAdES e consente di firmare digitalmente solo file PDF;
- XML, che identifica lo standard XAdES e consente di firmare digitalmente solo file XML;

1.3 VALORE DEI DOCUMENTI SOTTOSCRITTI CON FIRMA ELETTRONICA

Per quanto riguarda il valore dei documenti sottoscritti con i diversi tipi di firma elettronica, valgono le seguenti principali norme:

Regolamento eIDAS - Articolo 25

Effetti giuridici delle firme elettroniche

1) A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2) Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3) Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

CAD Art. 21
Documento informatico sottoscritto con firma elettronica.

1) Il documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e 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, (…) ha altresì 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. (…)

2-bis). Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale.

In sostanza, la normativa italiana (CAD) si adegua al principio europeo di non discriminazione sancito da eIDAS, per il quale un documento firmato elettronicamente non può essere ritenuto non ammissibile unicamente a motivo della sua forma elettronica o della tipologia di firma.

Tuttavia il CAD precisa quali sono gli atti che, per la loro natura, devono possedere necessariamente un tipo di firma di valore più elevato; pertanto, devono necessariamente essere firmati con firma **qualificata o digitale** i documenti di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, che sono:

1) i contratti che trasferiscono la proprietà di beni immobili;
2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
5) gli atti di rinunzia ai diritti indicati dai numeri precedenti;
6) i contratti di affrancazione del fondo enfiteutico;
7) i contratti di anticresi;
8) i contratti di locazione beni immobili per una durata superiore a nove anni;
9) i contratti di società [2247 ss.] o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;
10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato;
11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari;
12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti;

Per gli atti di cui al numero 13) del già citato articolo 1350, comma 1 codice civile (definiti come *gli altri atti specialmente indicati dalla legge*), invece, è ritenuta ammissibile anche la sottoscrizione con firma elettronica **avanzata**, oltre che con firma qualificata o digitale.

Rientrano tra gli atti di cui al numero 13) i seguenti:

- contratti di natura bancaria;
- atti costitutivi di associazioni o fondazioni;
- elezione di domicilio;
- convenzioni matrimoniali;
- accettazione/rinuncia/vendita di eredità:
- testamento;
- donazione;
- procura;
- riscatto di beni immobili;
- cessione di beni ai creditori;
- assunzione di lavoratori;
- atti costitutivi/fusioni di società;
- contratti di consorzio
- concessione/rinuncia/cancellazione di ipoteca;
- compromessi a seguito di controversie arbitrali;
- clausole compromissorie;
- contratti di costruzione navali/di aeromobili, modifiche e revoche agli stessi;
- atti relativi alla proprietà delle navi/degli aeromobili;
- concessione di ipoteche su navi/aeromobili;
- contratti di arruolamento del personale navigante

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 4

TIPOLOGIE DI FORMATI DEI DOCUMENTI

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1. I FORMATI

Qualsiasi oggetto digitale (ad es. un documento informatico) viene memorizzato sotto forma di file, ovvero come una sequenza di bit "0" o "1", considerati come un'entità unica dal punto di vista logico e fissati con una certa organizzazione fisica su un supporto di memorizzazione. Il documento informatico, come insieme di bit, esiste dunque solo in relazione ad un sistema informatico in grado di visualizzarlo o di trasferirne il contenuto su un supporto materiale (stampa), in modo che un essere umano possa prendere conoscenza del suo contenuto. Così, ad esempio, le informazioni contenute in un file creato con una data applicazione (word, excel, writer, calc, ecc.) vengono memorizzate secondo un particolare formato. Il formato dipende quindi dall'applicazione utilizzata nella fase di formazione del documento, di conseguenza, una determinata applicazione può interpretare correttamente e operare solo su file il cui formato è noto all'applicazione stessa. Diversamente la sequenza di bit memorizzata non avrebbe alcun significato e non sarebbe in alcun modo intelligibile se non se ne conoscesse il relativo formato.

Comunemente il formato di un file è identificato attraverso la sua estensione; si tratta di una serie di lettere, unita al nome del file attraverso un punto (ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft).

Oltre all'estensione, esistono altri metodi per identificare il formato di un file, tra cui i più impiegati sono i metadati espliciti, l'indicazione inserita nei tipi MIME e il cosiddetto "magic number", cioè i primi byte presenti nella sequenza binaria del file.

Per una trattazione più ampia delle varie tipologie di formati, si rimanda all'allegato 2 al DPCM 13 novembre 2014 in tema di documento informatico.

2. FORMATI DEI DOCUMENTI PRODOTTI DALL'ATENEO.

Alla luce delle considerazioni relative alle caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo, diffusione e idoneità alla conservazione, considerazioni ampliamente trattate nel citato Allegato 2 al DPCM 13/11/2014, l'Università degli Studi di Parma adotta, nella produzione dei propri documenti amministrativi informatici, il **formato PDF/A**. I principali applicativi di office automation permettono il salvataggio del documento redatto in modalità informatica in formato PDF/A.

A titolo esemplativo si riportano alcune prassi non corrette:

1) preparare il documento con applicativo di office automation (e.g. word), stampare il documento, firmarlo e successivamente scansionarlo in formato PDF;
2) preparare il documento con applicativo di office automation (e.g. word), stampare il documento, scansionarlo in formato PDF e successivamente firmare digitalmente il PDF ottenuto.

3. FORMATI DEI DOCUMENTI RICEVUTI

Per le medesime ragioni sopra esposte, si ritiene che il formato PDF/A sia da preferire anche in relazione al formato dei documenti amministrativi che altri soggetti inviano all'Ateneo. Pertanto, è opportuno che tutte le strutture organizzative dell'Ateneo indichino chiaramente ai soggetti con i quali intrattengono rapporti o negli avvisi di bandi, concorsi, selezioni, ecc. che il formato nel quale dovranno essere trasmessi i documenti è il PDF/A.

Tale decisione non configura una limitazione per i soggetti a cui è rivolta (studenti, aziende, altri enti, ecc.) in quanto i principali applicativi di office automation permettono di salvare direttamente nel formato PDF/A, e comunque sono disponibili applicazioni software gratuite che consentono di convertire i file in questo formato.

In una fase transitoria, in attesa che l'informazione si diffonda adeguatamente, si ritiene opportuno non rifiutare a priori i seguenti formati, in quanto indicati idonei per la conservazione nell'allegato 2 al DPCM 13/11/2014:

Nome formato	Estensioni
TIFF	.tif
JPG	.jpg, .jpeg
Open Office XML	.docx, .xlsx, .pptx
Open Document Format	.ods, .odp, .odg, .odb
XML	.xml
TXT	.txt

Tuttavia si raccomanda agli RPA di prestare attenzione all'utilizzo di formule o campi variabili nei suddetti formati, in quanto potrebbero compromettere il requisito di staticità/immodificabilità del documento stesso anche se sottoscritto con firma digitale.

A tal proposito, si riporta di seguito quanto disciplinato dall'Art. 4 comma 2 del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

3. Il documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21, comma 2, del Codice, se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 5

UTILIZZO FIRMA ELETTRONICA-DIGITALE

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1. UTILIZZO DELLA FIRMA ELETTRONICA[1]

L'Ateneo utilizza la firma digitale (la firma digitale è definita dal Decreto Legislativo 7 marzo 2005, n. 82 CAD – si tratta di una particolare firma elettronica) per tutti i documenti che produce per cui viene richiesta da norme particolari e/o per quelli che comportano responsabilità verso l'esterno.

Inoltre, la firma digitale può essere apposta anche sui documenti amministrativi aventi valenza interna all'Ateneo o endoprocedimentale, per i quali sia ritenuto opportuno, tenuto conto del contenuto del documento stesso, un livello più elevato di affidabilità.

1.1 FORMATI DI FIRMA ADOTTATI

Salvo sia richiesto diversamente da particolari normative o procedure informatiche, l'Ateneo ritiene opportuno apporre ai documenti amministrativi prodotti la firma digitale in formato PAdES.

Tale formato, che può essere apposto solamente a documenti prodotti in formato PDF (in particolare PDF/A) produce file firmati con estensione PDF e quindi leggibili dai software solitamente già presenti sui PC degli utenti; pertanto, la loro lettura da parte dei destinatari non richiede particolari operazioni di natura informatica, risultando particolarmente semplice.

Alla luce della Decisione di Esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015, i formati di firma utilizzati e accettati dall'Ateneo sono:

1) PAdES, che produce file con estensione PDF;
2) CAdES, che produce file con estensione P7M;
3) XAdES, che produce file con estensione XML.

[1] Alla luce dell'attività di analisi che verrà condotta, saranno in futuro introdotti specifici capitoli nei quali verranno elencati i documenti e i procedimenti per i quali, nell'ambito di appositi work flow, si potranno apporre firme elettroniche.

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 6

MODELLO COMUNE DI DOCUMENTO INFORMATICO

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1. MODELLO COMUNE DI DOCUMENTO

È riportato di seguito il template di carta intestata per lettere e Decreti/Determine del Direttore, realizzabile anche in bianco e nero.

UNIVERSITÀ DI PARMA
Via J. F. Kennedy, 6 - 43125 Parma
www.unipr.it

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 7

METADATI

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1 METADATI ADOTTATI

Per ogni tipologia di documento, i metadati minimi a norma di legge e quelli aggiuntivi scelti dall'Ateneo, sono richiesti e gestiti direttamente dall'applicativo in uso dall'Ateneo per la gestione del documento stesso

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 8

REPERTORI ATTIVI

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

1. REPERTORIO DEL REGISTRO DI PROTOCOLLO

Il repertorio del Registro di Protocollo è unico per il Dipartimento di Scienze Economiche e Aziendali con unica numerazione progressiva annuale.

2. REPERTORIO DEI DECRETI/DETERMINE DEL DIRETTORE

Il repertorio dei Decreti/Determine del Direttore è unico per il Dipartimento di Scienze Economiche e Aziendali con unica numerazione.

Il repertorio è esclusivamente in formato digitale.

I Decreti/Determine devono essere redatte in formato pdf/a e firmate digitalmente con firma pdf (Pades).

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 9

TITOLARIO DI CLASSIFICAZIONE

UNICO PER LE AREE

ORGANIZZATIVE OMOGENEE

DELL'UNIVERSITA' DEGLI STUDI DI PARMA

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

Si riporta nel seguito il Titolario di Classificazione Unico per le Aree Organizzative Omogenee *dell'Università degli Studi di Parma approvato con DR n. 2310 del 31/8/2016 in vigore dal 10/9/2016*

TITOLO I. Amministrazione

1. Normativa e relativa attuazione
2. Statuto
3. Regolamenti
4. Stemma, gonfalone e sigillo
5. Sistema informativo, sicurezza della informazione e sistema informatico
6. Protezione dei dati personali
7. Archivio
8. Trasparenza, relazioni con il pubblico
9. Strategie per il personale, organigramma e funzionigramma
10. Rapporti sindacali e contrattazione
11. Controllo di gestione e sistema qualità
12. Statistica e auditing
13. Elezioni e designazioni
14. Associazioni e attività culturali, sportive e ricreative
15. Editoria e attività informativo-promozionale
16. Onorificenze, cerimoniale e attività di rappresentanza
17. Politiche e interventi per le pari opportunità
18. Interventi a carattere politico, economico, sociale e umanitario

TITOLO II. Organi di governo, gestione, controllo, consulenza e garanzia

1. Rettore
2. Pro Rettori e Delegati
3. Senato Accademico
4. Consiglio di Amministrazione
5. Direttore Generale e Vice Direttore
6. Consiglio degli Studenti
7. Nucleo di Valutazione
8. Consiglio del personale tecnico-amministrativo
9. Collegio dei Revisori dei Conti
10. Collegio di disciplina
11. Comitato Unico di Garanzia
12. Comitato per lo Sport Universitario
13. Commissione paritetica docenti-studenti
14. Commissione Scientifica di Ateneo
15. Comitati Scientifici di Area
16. Commissioni e Gruppi di Lavoro
17. Consigliere di Fiducia
18. CRUI
19. CODAU
20. Comitato Regionale di Coordinamento
21. Consiglio
22. Giunta
23. Consiglio dei corsi di studio
24. Fondazione Università di Parma
25. Associazione Alumni e Amici dell'Università

TITOLO III. Didattica, ricerca, programmazione e sviluppo

1. Ordinamento didattico
2. Corsi di studio
3. Corsi ad ordinamento speciale
4. Corsi di specializzazione
5. Master
6. Corsi di dottorato
7. Corsi di perfezionamento e corsi di formazione permanente
8. Programmazione didattica, orario delle lezioni, gestione delle aule e degli spazi
9. Gestione di esami di profitto, di laurea e di prove di idoneità
10. Programmazione e sviluppo, comprese aree, macroaree e settori scientifico-disciplinari
11. Strategie e valutazione della didattica e della ricerca
12. Premi e borse di studio finalizzati e vincolati
13. Progetti e finanziamenti
14. Accordi per la didattica e per la ricerca
15. Rapporti con enti e istituti di area socio-sanitaria
16. Opere dell'ingegno, brevetti e imprenditoria della ricerca
17. Piani di sviluppo dell'Università
18. Cooperazione con paesi in via di sviluppo
19. Attività per conto terzi

TITOLO IV. Attività giuridico-legale

1. Contenzioso
2. Atti di liberalità
3. Violazioni amministrative e reati
4. Responsabilità civile, penale e amministrativa del personale
5. Pareri e consulenze

TITOLO V. Studenti e laureati

1. Orientamento, informazione e tutorato
2. Selezioni, immatricolazioni e ammissioni
3. Trasferimenti e passaggi
4. Cursus studiorum e provvedimenti disciplinari
5. Diritto allo studio, assicurazioni, benefici economici, tasse e contributi
6. Tirocinio, formazione e attività di ricerca
7. Servizi di assistenza socio-sanitaria e a richiesta
8. Conclusione e cessazione della carriera di studio
9. Esami di Stato e ordini professionali
10. Associazionismo, goliardia e manifestazioni organizzate da studenti o ex studenti

TITOLO VI. Strutture didattiche, scientifiche e di servizio

1. Poli
2. Scuole e strutture di raccordo
3. Dipartimenti
4. Strutture ad ordinamento speciale
5. Scuole di specializzazione
6. Scuole di dottorato
7. Scuole interdipartimentali
8. Centri
9. Sistema bibliotecario
10. Musei, pinacoteche e collezioni
11. Consorzi ed enti a partecipazione universitaria
12. Fondazioni

TITOLO VII. Personale

1. Concorsi e selezioni
2. Assunzioni e cessazioni
3. Comandi e distacchi
4. Mansioni e incarichi
5. Carriera e inquadramenti
6. Retribuzione e compensi
7. Adempimenti fiscali, contributivi e assicurativi
8. Pre-ruolo, trattamento di quiescenza, buonuscita
9. Dichiarazioni di infermità ed equo indennizzo
10. Servizi a domanda individuale
11. Assenze
12. Tutela della salute e sorveglianza sanitaria
13. Valutazione, giudizi di merito e provvedimenti disciplinari
14. Formazione e aggiornamento professionale
15. Deontologia professionale ed etica del lavoro
16. Personale non strutturato

TITOLO VIII. Finanza, contabilità e bilancio

1. Ricavi ed entrate
2. Costi e uscite
3. Bilancio
4. Tesoreria, cassa e istituti di credito
5. Imposte, tasse, ritenute previdenziali e assistenziali

TITOLO IX. Edilizia e territorio

1. Progettazione e costruzione di opere edilizie con relativi impianti
2. Manutenzione ordinaria, straordinaria, ristrutturazione, restauro e destinazione d'uso
3. Sicurezza e messa a norma degli ambienti di lavoro
4. Telefonia e infrastruttura informatica
5. Programmazione territoriale

TITOLO X. Patrimonio, economato e provveditorato

1. Acquisizione e gestione di beni immobili e relativi servizi
2. Locazione di beni immobili, di beni mobili e relativi servizi
3. Alienazione di beni immobili e di beni mobili
4. Acquisizione e fornitura di beni mobili, di materiali e attrezzature non tecniche e di servizi
5. Manutenzione di beni mobili
6. Materiali, attrezzature, impiantistica e adempimenti tecnico-normativi
7. Partecipazioni e investimenti finanziari
8. Inventario, rendiconto patrimoniale, beni in comodato
9. Patrimonio culturale – tutela e valorizzazione
10. Gestione dei rifiuti

TITOLO XI. Oggetti diversi

(Senza ulteriori suddivisioni in classi; affari che non rientrano nei precedenti titoli di classificazioni, neppure per analogia)

UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

ALLEGATO 10

ALLEGATO TECNICO PER IL SERVIZIO DI HOSTING DEL SISTEMA DI GESTIONE DOCUMENTALE

Redatto in riferimento a:

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEL DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI

REVISIONI

Nr	Data	Modifiche
00	27 agosto 2018	Prima stesura

SERVIZIO DI HOSTING CINECA
Allegato tecnico per il servizio hosting dei sistemi gestionali e business intelligence

1. Definizioni

Si tratta della predisposizione di risorse umane e tecnologiche da parte di CINECA a beneficio del COMMITTENTE in forma non esclusiva e con caratteristiche predefinite, affinché il COMMITTENTE possa utilizzare in modo completo ed esaustivo il Sistema.

Nel presente documento si utilizzerà la seguente terminologia:

- **Sistemi OLTP** (On Line Transaction Processing), per indicare i tipici sistemi applicativi gestionali, quali CIA, CSA, Esse3, U-GOV.
- **Sistemi OLAP** (On Line Analytical Processing), per indicare i sistemi applicativi di analisi, quali Datawarehouse di Ateneo.

2. Il valore del Servizio di Hosting al CINECA

Tramite il Servizio di Hosting di CINECA, il COMMITTENTE è in grado di gestire e utilizzare soluzioni applicative senza dover installare e mantenere presso la propria sede nessuna licenza software o sistema hardware o competenza specifica e quindi con modalità economicamente convenienti. I principali vantaggi che il COMMITTENTE ricava dal Servizio di Hosting sono:

- disponibilità dei servizi a costi ridotti, tramite un unico canone annuo;
- fruibilità facilitata per gli utenti;
- gestione totalmente in *outsourcing*, con risparmi relativi a personale interno dedicato, hardware e software di proprietà, gestione della connessione e della sicurezza;
- nessuna necessità di reperire personale formato per la manutenzione del sistema.

Il Data Center di CINECA è strutturato ed organizzato con l'obiettivo di fornire elevati standard qualitativi di servizio per quanto riguarda:

➢ Sicurezza fisica

Il Data Center possiede sistemi di rilevazione incendi, allagamenti e sistemi anti-intrusione. Sono sempre presenti o, comunque reperibili, i tecnici per risolvere ogni problema relativo alla conduzione degli impianti elettrici e di condizionamento.

In sintesi:

- i locali sono presidiati 24 ore al giorno, 7 giorni su 7;
- è presente un sistema anti-intrusione attivabile sulle recinzioni;
- le sale calcolatori sono protette da meccanismi di controllo accessi;
- è presente un sistema di rilevazione di incendi nei locali uffici e sale calcolatori;
- è presente un sistema di rilevazione allagamenti nelle sale calcolatori e nei magazzini;
- sono attivi controlli remoti dell'impianto di condizionamento e del gruppo di continuità per la gestione delle criticità eventuali.

L'accesso alla sala calcolatori è controllato dalla presenza di operatori, nel periodo diurno, e da personale di vigilanza durante la notte ed i fine settimana. In aggiunta, l'ingresso alla sala macchine è regolato da un sistema di controllo accessi basato su badge.

- Sicurezza e disponibilità dei sistemi e del networking

Gli apparati e le connessioni di rete sono ridondate. Tutti i sistemi critici sono alimentati attraverso sorgenti UPS/motogenerate. Per garantire i massimi livelli di sicurezza sono presenti sistemi di "anti-intrusione informatica" quali firewall e network ACL. Sono inoltre attivi sistemi antivirus con aggiornamento quotidiano.

- Protezione dei dati

Tutti i sistemi di storage utilizzano tecnologie di fault-tolerance (RAID) e sono sottoposti a politiche di backup/archive dei dati a breve e lungo termine. Allo scopo è presente una infrastruttura server di backup ridondata e dotata di libreria robotizzata per la gestione dei supporti (nastri magnetici). Per i sistemi OLTP, ad ulteriore protezione dei dati più critici, sono disponibili casseforti ignifughe, localizzate in zone distanti dalle sale calcolatori ed è attivo un sistema di replica remota per il deposito dei backup presso sito secondario, posto in altra area geografica.

3. Infrastruttura Tecnologica

Ove non diversamente specificato, le risorse sotto menzionate sono da considerarsi come non dedicate al singolo COMMITTENTE. La tipologia e le caratteristiche dei server e del software di base utilizzato potrebbe variare nel tempo in funzione delle evoluzioni tecnologiche.

Sistemi OLTP

L'infrastruttura tecnologica a supporto del servizio può comprendere una o più delle seguenti componenti, in base al tipo di hosting prescelto e all'applicazione ospitata:

Database Oracle: per gli ambienti operativi di produzione, il database Oracle (rel. 10 o successiva) è ospitato da un sistema in configurazione cluster ad elevata disponibilità (Server UNIX con capacità di fail-over delle istanze).

Application Server Farm: per gli ambienti operativi di produzione, lo strato di Application Server è implementato da una Server Farm basata su tecnologie Sybase Easerver oppure Oracle Application Server oppure JBOSS Application Server.

Terminal Server Farm: per gli ambienti operativi di produzione, lo strato di Terminal Server è implementato da una Server Farm basata su tecnologia Citrix Presentation Server.

Web Server Farm: per gli ambienti operativi di produzione, i servizi Web sono ospitati da Server Farm basate su tecnologia Apache/Tomcat, Apache/PHP ed Oracle Application Server oppure JBOSS Application Server.

Sistemi OLAP

L'infrastruttura dei servizi OLAP è dedicata a tali servizi e quindi vi è una completa separazione tra l'ambiente gestionale e l'ambiente analitico. L'utilizzo massivo dei sistemi di analisi non inficerà quindi le performance dell'ambiente transazionale.

Il Sistema si basa su tre livelli applicativi, ognuno dei quali caratterizzato da un'architettura di tipo cluster per garantire l'affidabilità del servizio.

- **Web Server**: web server in cluster (active/active) a livello di sistema operativo (load balancing + fail over automatico);

- **Application Server**: application server in cluster (active/active) a livello di applicativo OLAP (load balancing + fail over automatico);
- **DB Server**: DB server in cluster (active/passive) a livello di sistema operativo (fail over automatico).

Storage & Backup

Tutti i sistemi server dispongono di spazio disco su Storage Area Network e sfruttano l'infrastruttura di backup CINECA (STK SL8500 StorageTek StreamLine + IBM Tivoli Storage Manager).

Una copia dei dati utili alla erogazione del servizio di hosting viene conservata anche su un sito secondario (sito di Disaster Recovery). La frequenza di copia dei dati – ovvero la freschezza del dato – è detta RPO (Recovery Point Objective) ed è di 24H. CINECA, nell'ottica del continuo miglioramento, ogni anno provvede ad evolvere il servizio di Disaster Recovery con un RTO (Recovery Time Objective) di 72H ed un RPO (Recovery Point Objective) di 24H.

Il servizio di Disaster Recovery rispetterà le seguenti condizioni:

- Il sito primario del servizio di hosting è ubicato presso la sede CINECA di Casalecchio di Reno, mentre il sito secondario è ubicato nel territorio di Padova. CINECA si impegna a comunicare al COMMITTENTE, con adeguato preavviso, ogni variazione all'ubicazione dei siti.
- I dati del COMMITTENTE gestiti nell'ambito del servizio di hosting risiederanno all'interno del territorio italiano, nella fattispecie presso i siti primario e secondario previsti per il servizio. CINECA si impegna a comunicare al COMMITTENTE, con adeguato preavviso, ogni variazione all'ubicazione dei siti, pur garantendo sempre l'ubicazione interna al territorio italiano.
- CINECA garantirà i servizi per la riattivazione e il ripristino del sistema informativo primario, in presenza di un evento catastrofico, di una condizione di emergenza o di un disastro. I criteri per la definizione di tali eventi e la responsabilità per l'attivazione del Piano di Disaster Recovery per i servizi U-GOV in ambito al presente accordo, rimangono in carico a CINECA, che provvederà a darne visibilità al COMMITTENTE. A fonte di eventuali integrazioni fra l'applicazione informatica U-GOV e sistemi terzi del COMMITTENTE, CINECA si impegnerà nel coordinamento con il COMMITTENTE per la gestione in fase di emergenza (sia relativa a U-GOV che agli altri sistemi) dei rispettivi Piani di Disaster Recovery.
- CINECA verificherà costantemente la capacità della soluzione di Disaster Recovery di rispondere efficacemente alle situazioni di emergenza, assicurando un degrado delle prestazioni non superiore al 50%.
- CINECA si impegna ad eseguire test periodici (almeno una volta l'anno) per simulare il funzionamento del sito di Disaster Recovery in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo di produzione. Il test dovrà simulare una "vera" condizione di emergenza e/o di indisponibilità prolungata di tutte le apparecchiature del sito primario e, al fine di non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovrà predisporre copie dei dati ad uso esclusivo della simulazione, che saranno cancellate al termine delle prove.

Networking

L'utilizzo delle applicazioni in modalità disaster recovery presuppone una efficiente infrastruttura di connettività di rete, con banda adeguata al numero di utenti e di applicazioni utilizzate. La disponibilità dei servizi applicativi è ovviamente subordinata al corretto funzionamento delle linee di comunicazione tra CINECA e il COMMITTENTE. CINECA può fornire servizi di consulenza e supporto tecnico per individuare le soluzioni di connettività più adatte per il COMMITTENTE.

4. Licenze software

Sistemi OLTP

Sono comprese tutte le licenze del software di base (Sistema Operativo, Database, Application Server, Terminal Server, ecc.).

Sistemi OLAP

Sono comprese tutte le licenze del software di base (Sistema Operativo, Database, ecc.). Le applicazioni analitiche sono state sviluppate su Application Server Microstrategy. Le licenze di tale software non sono incluse nel servizio e dovranno pertanto essere acquistate, a cura del COMMITTENTE, direttamente dal rivenditore italiano: Microstrategy Italia.

5. Servizi di gestione

Viene fornita la completa conduzione dei server e dei servizi applicativi relativamente alle componenti di infrastruttura, sia per l'ambiente di produzione che per quello di pre-produzione disponibili nel sito primario che per l'ambiente di produzione disponibile nel sito di Disaster Recovery; in particolare:

- Gestione dell'hardware e del sistema operativo.
- Installazione e gestione delle componenti software di infrastruttura.
- Tuning dei sistemi e dell'infrastruttura.
- Monitoraggio dei servizi e dei sistemi.
- Salvataggio e ripristino dei dati.
- Assistenza sistemistica.

L'orario del presidio è da lunedì al venerdì, salvo festività, dalle ore 8.00 alle ore 19.00

Sistemi OLTP - Manutenzione programmata e straordinaria: per una corretta ed efficace conduzione di tutti i sottosistemi impiegati, saranno necessari brevi periodi di sospensione del servizio:

- Per la manutenzione ordinaria di sistema, verranno programmati periodi di sospensione dei servizi, con cadenza fissa trimestrale, posti al di fuori dal normale orario di lavoro degli utenti (uffici e sportelli di backoffice). I fermi per manutenzione ordinaria hanno solitamente una durata dell'ordine di 3-6 ore.
- Per la manutenzione straordinaria di sistema l'interruzione del servizio sarà sempre concordata preventivamente con il COMMITTENTE, secondo modalità volte a garantire l'integrità del sistema ed il minimo disservizio all'utenza finale.
- Ove possibile saranno unificati i periodi di manutenzione ordinaria e straordinaria.

Sistemi OLAP – Manutenzione programmata e straordinaria:

Eventuali interventi di CINECA per la manutenzione ordinaria e straordinaria dei sistemi saranno effettuati durante le ore lavorative previo avviso anticipato al COMMITTENTE. Qualora non fosse possibile, gli interventi saranno effettuati fuori dal normale orario di lavoro;

Sistemi OLAP – Caricamento periodico dei dati:

La periodicità dei caricamenti dati sarà concordata con il COMMITTENTE, in funzione del Data Mart o dei Data Mart implementati. La fascia oraria in cui saranno eseguiti i caricamenti è dalle 20.00 alle 8.00 dal Lunedì al Venerdì, mentre il Sabato e la Domenica sono possibili caricamenti anche durante le ore diurne. Il caricamento dei dati non sarà presidiato nei giorni di sabato, domenica, prefestivi e festivi e sarà verificato a partire dalle ore 9 del primo giorno lavorativo utile. Nel caso in cui un caricamento fallisca, dopo una prima analisi delle motivazioni, si cercherà nel più breve tempo possibile di ripristinare una situazione stabile e consistente.

Backup e Restore dati: per l'ambiente di produzione viene utilizzata una politica di backup giornaliero dei dati del DB (backup online + export). Su richiesta potranno essere archiviati singoli backup. Per i sistemi

OLTP, con cadenza mensile, vengono archiviati singoli backup (export). Per i sistemi **OLAP** tale archiviazione viene invece effettuata con cadenza semestrale.

Servizi di monitoraggio: Il CINECA gestisce il monitoraggio automatico per tutta l'infrastruttura di Hosting. Su richiesta possono essere attivati flussi di comunicazione via e-mail e/o SMS per la trasmissione degli eventi di alert verso il COMMITTENTE.

6. Servizi di supporto

Contatto Tecnico e comunicazioni di servizio: il COMMITTENTE si impegna ad individuare al suo interno una figura professionale che funga da referente tecnico nei confronti di CINECA. Per tutte le problematiche relative alla gestione sistemistica del servizio, che necessitino di una interazione tra CINECA ed il COMMITTENTE, tutte le comunicazioni dovranno avvenire esclusivamente tra il Referente Tecnico e le strutture di supporto di CINECA. Verranno attivati allo scopo canali di comunicazione telefonica ed e-mail. Il COMMITTENTE si obbliga a mettere a disposizione del CINECA le risorse necessarie e, quando richiesto, l'intervento da remoto per consentire il positivo esito dell'intervento. Si obbliga inoltre a mettere a disposizione il proprio personale in grado di comunicare al CINECA le informazioni eventualmente necessarie alla risoluzione del problema.

Supporto tecnico Hosting: sono tutte le attività eseguite da CINECA a fronte di segnalazioni di malfunzionamento del servizio, imputabili a cause di sistema. Il supporto per le problematiche applicative viene invece svolto dai rispettivi servizi di help-desk delle singole applicazioni. I sistemi Hw/Sw che implementano il servizio di Hosting sono opportunamente ridondati in modo da minimizzare il disservizio a fronte di guasti e malfunzionamenti. In alcuni casi, comunque, può rendersi necessario un intervento di ripristino del servizio da parte del personale Tecnico CINECA addetto alla conduzione dei sistemi. I livelli di servizio del supporto tecnico sono dettagliati più avanti in questo documento.

7. Modalità di accesso e fruizione

In tutti i casi sarà responsabilità del COMMITTENTE assicurare la corretta configurazione delle proprie stazioni di lavoro e della propria infrastruttura di rete per garantire l'accesso ai servizi in hosting presso CINECA in funzione delle modalità di accesso previste, che dipendono della tipologia di servizio.

Sistemi OLTP

Il servizio di Hosting prevede l'utilizzo di **una o più** delle seguenti modalità di fruizione, in base al tipo di hosting prescelto e all'applicazione ospitata:

Accesso Applicativo Web: secondo questa modalità gli utenti sono abilitati all'utilizzo dell'Applicativo mediante semplice web browser, con protocolli http/https.

Accesso Applicativo su Terminal Server: secondo questa modalità gli utenti sono abilitati all'utilizzo dell'Applicativo in modalità Terminal Server mediante il software Citrix-ICA-Client, che dovrà essere installato su tutte le stazioni di lavoro. La funzionalità di stampa prevista con questo tipo di accesso è quella fornita dal sottosistema Uniprint (produzione e delivery di files in formato PDF sulla stazione di lavoro dell'utente). CINECA fornisce il software Citrix+Uniprint; il Referente Tecnico ne esegue solamente la prima installazione, configurazione e verifica. I successivi aggiornamenti del Citrix-ICA-Client verranno eseguiti automaticamente dal sistema.

Accesso Applicativo su Application o DB Server: secondo questa modalità gli utenti sono abilitati all'utilizzo dell'Applicativo in diretta connessione con l'Application Server o DB server. Il Client Applicativo è installato sulla postazione di lavoro dell'utente. CINECA fornisce il software Applicativo; il Referente Tecnico ne esegue la prima installazione, configurazione e verifica. Collabora inoltre per rendere disponibili agli utenti i successivi aggiornamenti.

Accesso diretto al database: su richiesta del COMMITTENTE potranno essere attivati collegamenti diretti al database, solo per giustificati motivi e solamente da stazioni di lavoro del COMMITTENTE specificamente individuate per lo scopo. CINECA si riserva di valutare l'impatto che questi accessi hanno sul database e potrà eventualmente procedere alla loro sospensione in caso possano inficiare direttamente o indirettamente sulla qualità del servizio applicativo principale.

Sistemi OLAP

Il servizio di consultazione dati (analisi OLAP) è accessibile 24 ore su 24 con esclusione delle fasce orarie o nei giorni in cui avverranno i caricamenti del Data Warehouse, così come concordato con il COMMITTENTE. I servizi saranno accessibili mediante browser web standard (protocolli HTTP/HTTPS) o mediante l'utilizzo del client nativo Microstrategy, nel caso il COMMITTENTE ne abbia acquisito regolare licenza. Non è previsto alcun accesso diretto ai sistemi Database Server.

8. Integrazione con altri sistemi (solo per sistemi OLTP)

Per consentire l'integrazione applicativa con altri sistemi, eventualmente presenti presso il COMMITTENTE o presso CINECA possono essere attivate le seguenti modalità operative:

Flussi di integrazione su Database: per implementare eventuali flussi di interscambio di dati tra il database delle applicazioni in hosting CINECA e altri sistemi, attivi presso il COMMITTENTE, saranno utilizzati esclusivamente gli standard di comunicazione previsti da CINECA (es. accesso al DB CINECA con protocollo Oracle Net8) ed il COMMITTENTE dovrà adeguare i propri sistemi per uniformarsi allo standard. Ove invece non sia già definita una modalità standard di integrazione, la scelta della tecnologia e delle procedure da utilizzare dovrà essere concordata tra CINECA ed il COMMITTENTE in base alle esigenze applicative e di sistema. Il sistema esterno, che dialoga secondo gli standard stabiliti, è gestito interamente dal COMMITTENTE.

Oracle Dump: su richiesta del COMMITTENTE può essere fornito, con cadenza periodica, il dump Oracle (file di export), parziale o totale, del database di produzione. La periodicità dovrà essere compatibile con la regolare attività dei sistemi di produzione. Il file verrà depositato in una apposita area FTP o SFTP riservata, dalla quale il COMMITTENTE potrà prelevarlo via rete.

Accesso controllato al Database: possono essere definiti uno o più ruoli-utente con visibilità parziale e controllata allo schema DB. I sistemi che utilizzano l'accesso mediante questi ruoli sono gestiti interamente dal COMMITTENTE. CINECA si riserva di valutare l'impatto che questi accessi hanno sul database e potrà eventualmente procedere alla loro sospensione in caso possano inficiare direttamente o indirettamente sulla qualità del servizio applicativo principale.

Integrazione con altri sistemi CINECA: sarà cura di CINECA attivare flussi di comunicazione dati con gli altri sistemi di CINECA utilizzati dal COMMITTENTE (es: Posta Elettronica, DataMart, LDAP). Verranno attivati inoltre sistemi di monitor/alert per ciascuno dei suddetti flussi.

9. Livelli di servizio

Vengono specificati di seguito i livelli di servizio attesi.

Definizioni per le SLA di servizio	
Periodo di osservazione	Il periodo di osservazione per la misura degli SLA è fissato in **3** mesi solari consecutivi, a partire da gennaio, aprile, luglio, ottobre.
Finestra temporale di erogazione	Il servizio è fruibile con finestra temporale 24x7.

Definizioni per le SLA di servizio	
Disponibilità	Percentuale di tempo durante la quale i servizi sono disponibili all'utenza. Disponibilità = (1- (Periodo Disservizio / Periodo di osservazione)) * 100 Dove: • Disponibilità è espressa come valore percentuale. • Periodo Disservizio è la somma dei minuti di disservizio nel periodo di osservazione, calcolati rispetto alla finestra temporale di erogazione. • Periodo di osservazione è la durata in minuti del periodo di osservazione contrattuale. La disponibilità del servizio verrà calcolata al netto di: • fermi programmati e straordinari richiesti da CINECA • fermi programmati e straordinari richiesti dal COMMITTENTE • fermi dovuti a malfunzionamenti non attribuibili a CINECA
Sonda di monitoraggio	Il calcolo della Disponibilità si basa sulle misurazioni eseguite dall'infrastruttura di monitoraggio di CINECA. In particolare, per i servizi Web Based, viene eseguito un controllo automatico, accedendo ad una URL di servizio in grado di riportarne lo stato ed il servizio è considerato non disponibile se: • la URL interrogata ritorna un errore (errore HTTP, di connessione, ecc.) • la URL interrogata non ritorna risposta entro 15 secondi.

Livello di servizio TARGET	Obiettivo di qualità
Disponibilità	≥ 99.50%
Azioni contrattuali	Per ogni 0,1 % (ovvero 2,2 ore) di disponibilità inferiore all'obiettivo si applica una compensazione pari a 12 ore di servizio extra in estensione

Definizioni per le SLA di supporto	
Periodo di osservazione	Il periodo di osservazione per la misura degli SLA è fissato in 3 mesi solari consecutivi, a partire da gennaio, aprile, luglio, ottobre.
Finestra temporale di erogazione	Nei giorni feriali dalle ore 8 alle ore 19.
Classificazione disservizi	• **P1 - Incidente di Priorità 1 (bloccante):** il sistema è inaccessibile, l'utenza finale è totalmente impossibilitata alla fruizione del servizio oppure alcune specifiche funzioni fondamentali sono indisponibili per tutte le sessioni utente. (es: impossibilità di raggiungere la maschera del login). • **P2 - Incidente di Priorità 2 (non bloccante):** il sistema è accessibile, l'utenza finale può utilizzare il servizio, alcune specifiche funzioni NON fondamentali sono indisponibili per una o più sessioni utente.
Tempo di reazione (P1)	E' il tempo intercorrente tra il primo tentativo documentato di segnalazione del disservizio da parte del COMMITTENTE e l'emissione del Trouble Ticket, con relativa comunicazione (si considerano solo disservizi con livello di priorità pari a 1).
Tempo di reazione (P2)	E' il tempo intercorrente tra il primo tentativo documentato di segnalazione del disservizio da parte del COMMITTENTE e l'emissione del Trouble Ticket, con relativa comunicazione (si considerano solo disservizi con livello di priorità pari a 2).

SC_HOSTING03 - Pag. 7/8

Livello di servizio TARGET	Obiettivo di qualità
SLA di supporto	Incidenti: • Tempo di reazione (P1) < 30 minuti • Tempo di reazione (P2) < 120 minuti (nel 95% dei casi su base trimestrale per tutte le metriche sopra riportate)

Al fine di perseguire un continuo miglioramento del servizio, CINECA si propone di inserire già nella prossima convenzione con il COMMITTENTE (a meno che nel mentre non sia maturato il regolamento interconsortile) una valorizzazione in termini di estensione del servizio di hosting anche di eventuali sforamenti degli SLA di supporto usando degli indicatori, ed i relativi parametri, da individuare tra quelli previsti dai Lemmi di qualità ICT prodotti dalla Agenzia per l'Italia Digitale.

10. Limiti di applicabilità

- I livelli di servizio (SLA) sopra menzionati, non sono applicabili per eventuali situazioni di interruzione del servizio dovute a:

  a) indisponibilità nate da azioni non direttamente imputabili al CINECA;
  b) indisponibilità dei collegamenti di rete non direttamente imputabili al CINECA;
  c) indisponibilità dei collegamenti di rete del COMMITTENTE;
  d) problematiche hw/sw di base sulle postazioni di lavoro o server del COMMITTENTE

- UNIVERSITÀ si impegna a non apportare modifiche di qualunque natura al Sistema senza comunicazione al CINECA. Il CINECA si riserva la facoltà di non prendere in carico problemi causati da errati interventi tecnici effettuati da parte del COMMITTENTE.
- Risulta esplicitamente esclusa l'attività di assistenza applicativa o sistemistica per malfunzionamenti di hardware o software non fornito direttamente da CINECA.
- Il CINECA non assume alcuna responsabilità contrattuale o extracontrattuale con riguardo a prodotti hardware o software realizzati da terze parti. Le responsabilità relative ai prodotti di terze parti utilizzati dal CINECA per l'espletamento del servizio restano integralmente ed esclusivamente regolate in base alle garanzie prestate dai produttori.