Regione Siciliana
E.R.S.U. CATANIA
Ente Regionale per il Diritto allo Studio Universitario
Via Etnea n. 570 – 95128 Catania
Codice Fiscale 80006770871 - P. IVA 01264690874
Tel. 0957517910
www.ersucatania.it
Pec: protocollo@pec.ersucatania.it

Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi dell'E.R.S.U. di Catania

INDICE

1. PRINCIPI GENERALI

1.1. Premessa

Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 recante le "Regole tecniche per il protocollo informatico" di cui al decreto legislativo n. 82 del 2005, all'art. 3, comma 1, lettera d), prevede per tutte le amministrazioni di cui all'art. 2, comma 2, del D.Lgs. n. 82 del 2005 (Codice dell'Amministrazione Digitale) l'adozione del "**Manuale di gestione del protocollo informatico, dei documenti e dell'archivio**".

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, del suddetto DPCM "**descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi**".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile della gestione documentale, così come già previsto dall'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - Decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000.

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

Il protocollo informatico e il sistema di gestione documentale costituiscono il fulcro della struttura tecnologica ed organizzativa dell'Ente con riferimento alla gestione dei documenti, dei flussi documentali, dei processi e dei procedimenti amministrativi, nel rispetto della normativa vigente.

1.2. Ambito di applicazione del Manuale

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per la corretta gestione dei documenti, che comprende le attività di: formazione, registrazione, classificazione, fascicolazione e archiviazione e conservazione dei documenti.

Come prescritto dall'art. 5, comma 3 del DPCM 13 novembre 2013 Regole tecniche per il protocollo informatico, è pubblicato sul sito istituzionale dell'E.R.S.U. Catania.
Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

1.3 Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

● "amministrazione", E.R.S.U. Ente Regionale per il Diritto allo Studio Universitario- via Etnea 570, cap. 95128, Catania, C.F. 80006770871, protocollo@pec.ersucatania.it;

● "Testo Unico", il decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

● "Regole tecniche", il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico";

● "Codice", il decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale e ss.mm.ii.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

● AOO - Area Organizzativa Omogenea, l'Ente ha individuato una sola AOO che è composta dall'insieme di tutti i servizi dell'Ente, denominata **ERSU CATANIA**;

● CGD – Coordinatore della Gestione Documentale;

● MdG - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;

● RPA - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;

● RSP - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;

● SdP – Servizio di protocollo informatico;

● UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;

● UOB - Unità Operativa di Base;

● UU - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Ai fini delle definizioni del presente Manuale si è fatto riferimento alla seguente normativa e documentazione:

➢ Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

➢ Decreto legislativo 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale

➢ Decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii. e Regolamento (UE) 2016/679

➢ Legge 7 agosto 1990 n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi

➢ Legge 11 febbraio 2005, n. 15 - Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa;

➢ Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico;

➢ Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione;

➢ Decreto del Presidente del Consiglio dei Ministri 11 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni

➢ 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

➢ Quaderno 21 CNIPA, febbraio 2006 - Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle Pubbliche amministrazioni - Modello di riferimento

1.4. Aree organizzative omogenee (AOO), Unità Organizzative di Base (UOB) e modelli organizzativi

Ai fini della gestione unica e coordinata dei documenti l'Ente è costituito da un'unica Area organizzativa omogenea (AOO unica), formalmente definita con D.D.G. dell'assessorato regionale dei BB.CC.AA. e P.I. n. 756 del 28/11/2001

All'interno della AOO viene utilizzato un unico sistema di protocollazione per la registrazione della corrispondenza in entrata, in uscita ed interna.

Le Unità organizzative responsabili (UOB) sono individuate dall'Organigramma dell'Ente (Allegato 1 - Organigramma dell'E.R.S.U. Catania).

1.5. Servizio archivistico dell'E.R.S.U. Catania per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi

Nella AOO è istituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il **Direttore**, Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP). Le attività afferenti al Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi, sono coordinate **dal Direttore**, il Coordinatore della gestione documentale (di seguito VI)

Ai sensi dell'art. 5, comma 3 del DPCM 13 novembre 2013 Regole tecniche per il protocollo informatico sono compiti del Responsabile del Servizio:

➢ predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;

➢ proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;

➢ predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;

➢ Sono inoltre compiti del Servizio:

− abilitare gli addetti dell'amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.);

− garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;

− garantire la corretta produzione e conservazione del registro giornaliero di protocollo;

− curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

− conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;

− garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;

− autorizzare le operazioni di annullamento delle registrazioni di protocollo;

− aprire e chiudere il registro di emergenza.

1.6 Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, entro le ore 12.00 del giorno successivo, il contenuto del registro informatico di protocollo, viene inviato in conservazione.

1.7 Tutela dei dati personali

L'amministrazione, titolare dei dati di protocollo e dei dati personali, comuni, sensibili e/o giudiziari, contenuti nella documentazione amministrativa di propria competenza, ha ottemperato al dettato del **Decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii., e del Regolamento (UE) 2016/679 .**

1.8 Caselle di Posta Elettronica

L'AOO si è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza - **protocollo@pec.ersucatania.it-** sia in ingresso che in uscita. Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOB) che ad essa fanno riferimento. In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione ha assegnato ai propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, una casella di posta elettronica istituzionale.

1.9 Sistema di classificazione dei documenti

Con l'inizio dell'attività operativa del protocollo informatico, è stato adottato un unico Titolario di classificazione per l'archivio centrale unico dell'amministrazione. Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO. Esso consente di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico. Al fine di agevolare e normalizzare, da un lato, la classificazione archivistica e, dall'altro, l'assegnazione per competenza, sul SdP è stato predisposto un elenco degli Uffici Utente e dei dipendenti

unitamente a quello di classificazione. L'elenco è una guida rapida di riferimento, in ordine alfabetico che, sulla base del Titolario, permette l'immediata individuazione della classificazione e delle competenze.

1.10 Formazione

Nell'ambito dei piani formativi richiesti a tutte le pubbliche amministrazioni sulla formazione e la valorizzazione del personale, l'Amministrazione stabilisce periodicamente percorsi formativi, specifici e generali, che coinvolgono tutte le figure professionali.

1.11 Accreditamento dell'AOO all' IPA

L'AOO, come accennato, si è dotata di una casella di posta elettronica certificata attraverso la quale trasmette e riceve documenti informatici soggetti alla registrazione di protocollo. Tale casella è affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura almeno una volta al giorno della corrispondenza ivi pervenuta.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), in data 02/08/2013, fornendo le informazioni che individuano l'amministrazione e l'articolazione delle sue AOO. Il codice identificativo dell'amministrazione è stato generato e attribuito autonomamente dall'amministrazione (rseu_087). L'IPA è accessibile, tramite il relativo sito internet, a tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità dell'indirizzo di posta elettronica indicato. Con la stessa tempestività, l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.12 Dematerializzazione dei procedimenti amministrativi della AOO

L'amministrazione ha in fase di prossima realizzazione procedure tali da consentire, in coerenza con le disposizioni normative e regolamentari in materia, che nella AOO siano prodotti, gestiti, inviati e conservati solo documenti informatici. È prevista la riproduzione su carta degli originali informatici firmati e protocollati solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti informatici. Gli eventuali documenti cartacei ricevuti, dopo registrazione e segnatura di protocollo, sono sottoposti al processo di scansione per la loro dematerializzazione.

1.13 Sistema di protocollo informatico unico e strumenti per il suo funzionamento

L'Ente, avendo individuato un'unica AOO, si serve di un unico sistema di protocollo informatico denominato Easy Prot.

Il protocollo informatico unico è lo strumento attraverso il quale l'Ente garantisce l'effettiva ricezione e trasmissione dei documenti.

Con la messa a regime di tale sistema è cessata di fatto la necessità di mantenere tutti i cosiddetti protocolli interni (protocolli di settore, servizio, ufficio, etc., protocolli multipli, protocolli del telefax, etc.) o altri sistemi di registrazione diversi dal protocollo unico, che sono stati o saranno eliminati con i tempi e le modalità stabilite al paragrafo seguente.

2. PIANO DI SICUREZZA

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

2.1. Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

➢ i documenti e le informazioni trattati dall'Ente siano resi disponibili, autentici e integri;

➢ i dati personali, i dati sensibili e quelli giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2.2. Contesto di riferimento

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

➢ le politiche generali e particolari di sicurezza da adottare all'interno dell'Ente

➢ le modalità di accesso al sistema di protocollo e gestione documentale

➢ le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico

➢ le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

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

➢ protezione periferica della Intranet dell'amministrazione;

➢ protezione dei sistemi di accesso e conservazione delle informazioni;

➢ assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;

➢ piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;

➢ conservazione, a cura dei Servizi informatici, delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;

➢ gestione delle situazioni di emergenza informatica attraverso risorse qualificate;

➢ impiego e manutenzione di un adeguato sistema antivirus;

➢ uso di codici identificativi (o altre soluzioni) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli inintelligibili a chi non è autorizzato ad accedervi;

➢ impiego di idonee misure di sicurezza anche nel caso di supporti analogici contenenti banche di dati sensibili e giudiziari;

➢ archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultabili in caso di necessità dalle forze dell'ordine.

2.3. Formazione dei documenti - aspetti di sicurezza

Il documento informatico, identificato in modo univoco e persistente, è memorizzato nel sistema di gestione informatica dei documenti in uso nella AOO che ne garantisce l'inalterabilità, la riservatezza e la fruibilità da parte di persone dotate di adeguate autorizzazioni. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 del DPCM 13 novembre 2014 in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità.

2.4. Gestione dei documenti informatici - aspetti di sicurezza

I documenti dell'Ente vengono gestiti attraverso Il sistema di protocollo e gestione documentale Easy Prot.

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato nelle modalità descritte nel precedente paragrafo 2.2.

Il sistema di gestione informatica dei documenti:

➢ garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

➢ assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

➢ fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

➢ consente il reperimento delle informazioni riguardanti i documenti registrati;

➢ permette, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;

➢ garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.4.1. Componente organizzativa della sicurezza

Tale componente consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte dal sistema informatico Easy Prot. In tale contesto la gestione della sicurezza si realizza con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia e con attività di controllo e verifica essenziali ad assicurare l'efficacia nel tempo del sistema informatico.

Nella conduzione del sistema informativo sono responsabili del trattamento dei dati i dirigenti preposti ad ogni settore dell'Ente.

2.4.2. Componente fisica e infrastrutturale della sicurezza

Il controllo degli accessi fisici alle risorse della sede del Centro servizi è regolato secondo i seguenti principi:

● l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;

● i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale;

● i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'erogatore del servizio autorizzato a quel livello di protezione;

● ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo con sistemi di autenticazione forte;

● gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;

● il personale della sede ha l'obbligo di utilizzare il badge sia in ingresso che in uscita dalla sede stessa.

2.4.3. Componente logica della sicurezza

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

Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale Easy Prot, è stata realizzata attraverso:

➢ identificazione e autenticazione utente

➢ profilazione degli accessi (ACL)

➢ politica antivirus

➢ firma digitale

➢ monitoraggio sessioni di lavoro

➢ disponibilità del software e dell'hardware

2.4.4. Gestione delle registrazioni di protocollo e di sicurezza

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

Le registrazioni di sicurezza possono essere costituite:

➢ dai log di sistema generati dal sistema operativo

➢ dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall)

➢ dalle registrazioni di Easy Prot

2.4.5. Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni dell'Ente l'accesso ai servizi previsti, mediante l'adozione di un insieme di misure organizzative e tecnologiche.

Gli utenti interni autorizzati ad utilizzare il software Easy Prot, operano secondo quanto segue:

➢ ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati ai fini istituzionali;

➢ ogni utente è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali.

➢ ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. É vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus;

➢ I dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative;

➢ La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare con frequenza opportuna i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti;

➢ Tutti i dati sensibili riprodotti su supporti magnetici (e informatici, ndr.), devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto;

➢ L'account del sistema Easy Prot è costituito da un codice identificativo personale (username) e da una parola chiave (password);

➢ La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.

2.5. Trasmissione e interscambio dei documenti informatici

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

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all' interno della AOO o ad altre AOO, contengono soltanto le informazioni relative a stati, fatti e qualità Manuale di gestione del protocollo informatico, dei documenti e degli archivi personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

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

● accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare;

● l'integrità del messaggio e del suo contenuto;

● tracciamento delle attività nel file di log della posta;

● gestione automatica delle ricevute di ritorno.

Per garantire alla AOO la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

2.5.1. All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

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

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete. Il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

2.5.2. All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

Gli uffici organizzativi di riferimento (UOB) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005 concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

2.6 Accesso ai documenti informatici

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

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

Queste, in sintesi, sono:

● consultazione, per visualizzare in modo selettivo, le registrazioni di protocollo 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 RSP. Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori delle AOO che per gli utenti delle AOO. Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il SdP fruito dall'AOO:

● consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti;

● assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Tali registrazioni sono protette 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). Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo UOB, o agli Uffici Utente (UU) ad esso subordinati. Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

2.6.1. Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'AOO.

Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

● gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento)

● la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del login.

2.6.2. Accesso al registro di protocollo per utenti interni alla AOO

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

● liste di competenza, gestite dall'amministratore di AOO;

● ruoli degli utenti, gestiti dall'amministratore di ente (amministrazione), per la specificazione delle macro-funzioni alle quali vengono abilitati;

● protocollazione "particolare o riservata", gestita dall' amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare. L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo ed assegnarlo per competenza ad un utente assegnatario.

Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e al Responsabile di protocollo che ha il permesso applicativo di visualizzazione protocollazione riservata (permesso associato al ruolo). Tutti gli altri

utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo del protocollo (ad esempio : classificazione).

2.6.3. Utenti esterni alla AOO - Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss del d.lgs 7 marzo 2005 n. 82.

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

● numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;

● identificazione dell'UU di appartenenza del RPA.

2.6.4. Utenti esterni alla AOO - Privati

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

3. MODALITÀ DI FORMAZIONE DEI DOCUMENTI

3.1. I documenti dell'E.R.S.U. Catania

I documenti dell'E.R.S.U. Catania (d'ora in poi chiamati semplicemente documenti) sono quelli prodotti (spediti e ricevuti), in uno dei modi previsti dalla normativa vigente, dagli organi ed uffici dell'Ente medesimo nello svolgimento della loro attività istituzionale.

In ottemperanza a quanto indicato dal Codice dell'Amministrazione Digitale, che prevede l'uso delle tecnologie dell'informazione e della comunicazione per organizzare la propria attività amministrativa, l'E.R.S.U. Catania sta progressivamente evolvendo verso la formazione, gestione, e trasmissione dei documenti informatici.

Ciò premesso, il documento amministrativo va distinto in:

➢ documento analogico

➢ documento informatico

Tutti i documenti originali, indipendentemente dal loro supporto, sono tra loro connessi da speciale vincolo originario, necessario e determinato e costituiscono l'archivio dell'ente.

3.2. Formazione dei documenti - aspetti diplomatici

I documenti prodotti dall'Ente indipendentemente dalla forma nella quale sono redatti, devono sempre riportare gli elementi essenziali, elencati di seguito.

Deve essere curata, per quanto possibile, la standardizzazione della forma e dei contenuti dei documenti, attenendosi a formulari tipici, sottoposti ad approvazione del dirigente competente.

3.2.1. Elementi informativi essenziali dei documenti prodotti

I documenti in uscita devono riportare le seguenti informazioni, organizzate per blocchi logici:

1. Individuazione dell'autore del documento - logo dell'Ente e dicitura "E.R.S.U. Catania" nelle forme stabilite dall'amministrazione - Unità Organizzativa Responsabile con eventuale indicazione del servizio e dell'ufficio - Indirizzo completo: via/piazza, numero civico, cap, città - Codice fiscale e partita IVA - Numero di telefono ed eventuale fax - Indirizzo istituzionale di posta elettronica - Indirizzo di posta elettronica certificata - Orario di apertura al pubblico

2. individuazione e descrizione del documento: - Numero di protocollo - Data di protocollo (giorno, mese, anno) - Eventuale numero del repertorio - Indice di classificazione: titolo/classe/numero di fascicolo - Numero e descrizione degli allegati - Numero e data del documento cui si risponde - Oggetto del documento

3. individuazione del destinatario del documento (se è un documento in uscita): - Cognome e nome (per le persone)/ Denominazione (per gli enti e le imprese) / UOB (per i documenti interni) - A seconda dei casi: - Indirizzo completo: via/piazza, numero civico, cap, città - Indirizzo informatico (Pec…)

4. individuazione del RPA: - Cognome, nome e qualifica del Responsabile del procedimento amministrativo - Sottoscrizione (firma autografa o digitale)

3.3. Formazione dei documenti - aspetti operativi generali

I documenti dell'Ente sono prodotti generalmente con adeguati sistemi informatici o in alternativa in modalità analogica.

Ogni documento amministrativo:

➢ tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto

➢ è riferito ad un solo protocollo

➢ fa riferimento ad uno o più fascicoli

3.4. Formazione del documento amministrativo analogico

Per documento analogico si intende la rappresentazione non informatica di atti, fatti, o dati giuridicamente rilevanti. Si definisce "originale" il documento nella sua redazione definitiva corredato degli aspetti diplomatici sopra descritti. Un documento analogico può essere convertito in documento informatico ai sensi dell'art. 22 del D.lgs. 82/2005.

3.5. Formazione del documento informatico e del documento amministrativo informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Il documento informatico viene formato mediante una delle seguenti principali modalità:

➢ redazione tramite l'utilizzo di appositi strumenti software;

➢ 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;

➢ registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

➢ 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 interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:
➢ sottoscrizione con firma digitale, ovvero con firma elettronica qualificata

➢ apposizione di una validazione temporale

➢ trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa

➢ memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza

➢ versamento ad un sistema di conservazione

Al documento informatico immodificabile e ai documenti soggetti a registrazione particolare vengono associati i metadati che sono stati generati durante la sua formazione.

L'insieme minimo dei metadati è costituito da:

A. Identificativo univoco e persistente

B. Riferimento temporale

C. Oggetto

D. Soggetto che ha formato il documento

E. Destinatario

F. Impronta del documento informatico

G. Metadati aggiuntivi stabiliti dall'Ente a fini gestionali e conservativi

Nel caso specifico del documento amministrativo informatico l'insieme di metadati minimi è costituito da:

A. Numero di protocollo

B. Data di protocollo

C. Mittente – destinatario

D. Oggetto

E. Data e protocollo del documento ricevuto, se disponibili

F. Impronta del documento informatico

G. Metadati aggiuntivi stabiliti dall'Ente a fini amministrativi, gestionali e conservativi

3.5.1. La firma elettronica (avanzata, qualificata e digitale)

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con processi di firma elettronica conformi alle disposizioni dettate dalla normativa vigente.

Per l'apposizione della firma digitale, l'Ente si avvale dei servizi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale.

I documenti informatici prodotti dall'Ente indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti nel formato standard PDF/A, al fine di garantirne l'immodificabilità e la corretta archiviazione.

La firma digitale viene utilizzata dall'Ente come forma di sottoscrizione per garantire i requisiti di integrità, riservatezza e non ripudiabilità nei confronti di entità esterne.

Le verifiche delle firme digitali dei documenti prodotti o ricevuti avviene attraverso l'utilizzo di software rilasciati gratuitamente, secondo la normativa, da enti certificatori.

Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna l'Ente, nella propria autonomia organizzativa, adotta forme diverse dalla firma digitale previste dal DPCM 22 febbraio 2013.

3.5.2. La marcatura temporale

Per tutte le casistiche per cui la normativa prevede l'apposizione di un riferimento o validazione temporale, l'Ente adotta almeno una delle seguenti modalità di marcatura:

➢ registrazione di protocollo

➢ posta elettronica certificata

➢ eventuale sistema di marcatura temporale, nei casi in cui non sia possibile utilizzare uno di quelli precedenti

3.5.3. Tipologie di formato del documento informatico

L'Ente, in considerazione di quanto previsto dal DPCM 3 dicembre 2013 in materia di conservazione, al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, adotta i seguenti formati:

FORMATO	ESTENSIONE	STANDARD DI RIFERIMENTO
PDF - PDF/A	.pdf	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4)

		ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	ISO 12639 ISO 12234
JPG	.jpeg, .jpg	ISO/IEC 10918:1
Office Open XML (OOXML)	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008
Open Document Format	.odt, .ods, .odp, .odg, .odb	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
XML	.xml , derivati da XML: .svg	ISO 8879 - SGML Specifiche W3C 27
TXT	.txt	/
formati messaggi di posta elettronica	.eml	RFC 2822 - MIME RFC 1847 - S/MIME
AutoCAD DXF	.dxf	proprietario ma con specifiche rilasciate da Autodesk
M4a	.m4a, .m4b, .mp4	ISO/IEC 14496-14
MP3	.mp3	ISO/IEC 11172-3 ISO/IEC 13818-3
WAV	.wav	rilasciato da IBM e Microsoft. estensione del Resource Interchange File Format (.RIFF)

Eventuali integrazioni al presente elenco vengono definite in considerazione di specifiche previsioni normative o tecniche.

4. MODALITÀ DI SCAMBIO DEI DOCUMENTI

Il presente capitolo fornisce indicazioni per lo scambio di documenti all'interno ed all'esterno dell'AOO. Tutti i documenti pervenuti all'Ente devono essere registrati, segnati, classificati e smistati alla UOB di competenza contestualmente alla loro ricezione nella stessa giornata in cui sono pervenuti.

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

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

• entrata

• uscita

• interno

4.1. Documenti in entrata

4.1.1. Ricevuti o prodotti su supporto analogico

I documenti ricevuti su supporto analogico possono essere recapitati attraverso:

Il Protocollo generale provvede dopo l'assegnazione da parte del Direttore o di chi ne fa la veci immediatamente alla registrazione a protocollo attraverso il sistema di protocollo informatico e gestione documentale e alla segnatura dei singoli documenti dando priorità a quelli individuabili come urgenti.

➢ Fax: I documenti ricevuti tramite fax sono da considerarsi a tutti gli effetti analogici, poiché solo la loro modalità di trasmissione è telematica.

➢ Brevi Manu: consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata allo sportello del Protocollo generale o agli altri uffici di protocollo delle UOB aperti al pubblico durante l'orario di apertura. Gli operatori provvedono alla registrazione, segnatura e scansione dei documenti, con relativo smistamento alle UOB di competenza nello stesso giorno di ricezione.

Su richiesta dell'interessato viene rilasciata apposita ricevuta della avvenuta registrazione mediante il programma di protocollo informatico o, in alternativa, viene apposta la segnatura di protocollo sulla copia già in possesso dell'utente apponendo la dicitura "copia per l'utente". In tutte e tre le casistiche avviene un processo di scansione e inserimento all'interno del sistema di protocollo informatico.

4.1.2. Ricevuti o prodotti su supporto informatico

I documenti informatici possono essere recapitati/trasmessi tramite:

➢ Caselle di posta elettronica istituzionale: la casella istituzionale dell'Ente è protocollo@ersucatania.it; inoltre sono istituite le caselle di posta elettronica istituzionale dei rispettivi settori, pubblicate sul sito istituzionale www.ersucatania.gov.it.

➢ Posta elettronica certificata: la casella PEC dell'Ente è protocollo@pec.ersucatania.it;

➢ Canali Web: l'E.R.S.U Catania è dotato di un portale web, raggiungibile dall'indirizzo www.ersucatania.gov.it, attraverso il quale è possibile presentare istanze e richieste.

➢ Eventuali canali informativi cooperativi.

4.2. Documenti inviati

Le comunicazioni verso i privati avvengono sia attraverso i canali analogici che informatici, le comunicazioni verso le altre pubbliche amministrazioni avvengono di norma mediante l'uso dei canali informatici.

4.2.1. Inviati su supporto analogico

I documenti analogici sono trasmessi attraverso:

A. Posta convenzionale o posta raccomandata

B. Brevi Manu

C. Notifica

Il documento in uscita viene normalmente, sottoscritto dal Responsabile del procedimento amministrativo e registrato nel sistema di protocollo informatico e l'originale spedito.

4.2.2. Inviati su supporto informatico

I documenti informatici sono trasmessi attraverso:

A. Caselle di Posta elettronica

B. Posta elettronica certificata

Se il documento cartaceo è inviato tramite posta elettronica certificata o canali digitali, viene redatto in un unico esemplare, sottoscritto, registrato, acquisito tramite scansione nel sistema di protocollo, dal quale viene inoltrato alla posta elettronica certificata del destinatario. Trattenuto presso il produttore e inserito nel fascicolo relativo all'affare o al procedimento amministrativo trattato.
Se il documento è informatico viene inviato tramite posta elettronica certificata o canali digitali, viene redatto tramite un software di elaborazione testi, sottoscritto con firma digitale, registrato, acquisito nel sistema di protocollo e di gestione documentale e inoltrato alla posta elettronica certificata del destinatario.

4.3. Documenti interni

I documenti interni, cioè i documenti prodotti e destinati all'interno dell'AOO dell'Ente, sono formati con tecnologie informatiche **o in formato cartaceo**.

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

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione. L'Ente utilizza il sistema di protocollo informatico e di gestione documentale Easy Prot.

5.1. Registrazione dei documenti

Tutti i documenti dell'Ente, dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell'Ente, con le modalità e le eccezioni di seguito illustrate.

La registrazione è l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, alla forma, all'autore e alla modalità di trasmissione di un documento.

Tale operazione serve a identificare in modo univoco un documento individuandone data, forma e provenienza certa.

Anche i documenti soggetti a repertoriazione, forma particolare di registrazione, possono essere registrati sul protocollo informatico unico dell'Ente. La registrazione a protocollo riguarda il singolo documento; non può riguardare per alcun motivo il fascicolo, in quanto è vietata la registrazione cosiddetta "sintetica". Quindi il numero di protocollo individua un singolo documento.

5.2. Registro di protocollo

Il registro di protocollo, è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

Nell'ambito della AOO dell'Ente il registro di protocollo è unico e la sua numerazione, unica, progressiva e costituita da almeno sette cifre numeriche, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

La documentazione che non è stata registrata viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato, salvo casi inevitabili di invii multipli da parte del mittente.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici. Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Ai sensi dell'art. 7 comma 5 del DPCM 3 dicembre 2013, il registro giornaliero di protocollo è trasmesso entro alla giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

5.3. Elementi della registrazione di protocollo

Gli elementi obbligatori, in quanto giuridicamente rilevanti della registrazione a protocollo sono:

- ➢ data di registrazione
- ➢ numero di protocollo
- ➢ mittente per il documento in arrivo/ destinatario per il documento in partenza
- ➢ oggetto
- ➢ indice di classificazione

➢ modalità di trasmissione

➢ tipologia del documento

Gli elementi non obbligatori, ma funzionali qualora disponibili sono:

➢ numero di protocollo del documento ricevuto

➢ data del documento ricevuto

➢ numero degli allegati

➢ annotazioni

5.4. Modalità di registrazione di protocollo

I documenti pervenuti all'Ente da altri soggetti giuridici sono registrati una sola volta, salvo casi di invii multipli non individuabili da parte del mittente, come documenti in entrata.

I documenti inviati dall'Ente ad altri soggetti giuridici sono registrati una sola volta come documenti in uscita. I documenti interni formali, inviati da una UOB ad un'altra UOB all'interno dell'Ente (oppure da un ufficio all'altro all'interno della stessa UOB), devono essere registrati a protocollo una sola volta dalla UOB mittente come documenti interni. In seguito alla registrazione i documenti analogici vengono acquisiti nel sistema di protocollo tramite procedura di scansione; I documenti informatici vengono acquisiti nel sistema di protocollo attraverso le modalità descritte nel capitolo 4. In entrambi i casi vengono assegnati alla UOB competente. Il responsabile di ciascuna UOB prende atto tramite il sistema informatico che gli sono stati smistati dei documenti; provvede sotto la propria responsabilità e con cadenza quotidiana a prendere in carico il documento dalla scrivania virtuale di Easy Prot.

5.5. La segnatura di protocollo

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

Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste ai sensi del DPCM 3 dicembre 2013 sono:

A. codice identificativo dell'amministrazione

B. codice identificativo dell'area organizzativa omogenea

C. codice identificativo del registro

D. progressivo registrazione

E. data di registrazione

Ulteriori informazioni previste sono:

A. indicazione della UOB dell'Ente responsabile del documento prodotto.

B. anno

C. titolo

I dati relativi alla segnatura di protocollo di un documento trasmesso da una AOO sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale. All'interno del file XML devono essere contenute anche le seguenti informazioni minime:

A. l'oggetto

B. il mittente

C. il destinatario o i destinatari

La segnatura di protocollo permette di realizzare l'interoperabilità tra i sistemi di gestione informatica dei documenti di amministrazioni diverse, automatizzando, fino al massimo livello possibile, la registrazione di protocollo di documenti informatici provenienti da altri sistemi interoperabili. Qualora il documento venga prodotto su formato analogico al termine della registrazione la segnatura viene apposta tramite etichetta (le cui informazioni sono il risultato dell'estrazione delle informazioni minime contenute nella segnatura informatica). Questa riporterà il numero e la data di protocollo, la classificazione, la UOB e un codice a barre che permetterà l'associazione del documento acquisito mediante lo scanner alla registrazione di protocollo.

5.6. Documenti soggetti a registrazione particolare (Repertoriazione)

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'art. 53, comma 5 del D.P.R. 445/2000.

Tale tipo di registrazione particolare consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione e la fascicolazione; anche questi documenti appartengono al complesso archivistico dell'Ente e concorrono al popolamento del sistema di gestione documentale dell'Ente nell'ottica di una gestione uniforme e coordinata.

Questi documenti costituiscono delle serie di interesse archivistico e sono collegate a registri o repertori che contengono almeno le seguenti informazioni:

➢ tipologia del registro o repertorio

➢ numero di registro o repertorio (cronologico e progressivo)

➢ data

➢ elementi identificativi dell'atto (soggetto o soggetti; oggetto)

➢ eventuali dati di classificazione e di fascicolazione

➢ annotazioni

5.7. Procedure specifiche nella registrazione di protocollo

5.7.1. Protocolli riservati

Sono previste particolare forme di riservatezza e di accesso controllato al protocollo unico per:

➢ documenti relativi a vicende di persone o a fatti privati o particolari (dati sensibili, come definiti dalla D. lgs. 196/2003 **e** ss.mm.ii e dal Regolamento (UE) 2016/679

➢ documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite dalla Legge 241/1990, art. 24).

I documenti registrati con tali forme appartengono al cosiddetto protocollo riservato, costituito dalle registrazioni sul protocollo informatico unico dell'Ente il cui accesso è consentito solamente alle persone autorizzate, in rapporto alle tipologie di procedimento amministrativo o alle tipologie documentarie dalle stesse trattate.

Le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del sistema di protocollo informatico a cura **del CDG.**

Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato, comprese la registrazione, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti e procedimenti amministrativi.

5.7.2. Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni.

Tra le eccezioni si annoverano i documenti soggetti a registrazione particolare di cui al precedente paragrafo 5.6. e i documenti di cui all'art. 53, comma 5 del D.P.R. 445/2000.

5.7.3. Annullamento delle registrazioni di protocollo

Le informazioni non modificabili della registrazione a protocollo sono annullabili ai sensi dell'art. 54 del DPR 445/2000 ma devono rimanere memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile del servizio archivistico.

La procedura di annullamento di una registrazione è di competenza dell'Ufficio Protocollo Generale che, con cadenza mensile, trasmette un elenco al **CDG.**

5.8. CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

5.8.1. Lettere anonime

La lettera anonima proveniente tramite i canali postali, una volta aperta e attestata l'assenza di ogni riferimento al mittente, viene posta all'attenzione del Direttore o di persona dallo stesso delegata, che fornirà istruzioni in merito al suo trattamento agli addetti del Protocollo, i quali provvederanno secondo le indicazioni ricevute, alla sua registrazione (indicando nel campo mittente "anonimo") ovvero alla sua eliminazione.

Nel caso in cui si effettui la registrazione a protocollo, la procedura prevede l'utilizzo del protocollo riservato, per limitare la visibilità del documento anonimo alla UOB o agli organi interessati.

5.8.2. Lettere prive di firma

Le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali. La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. È poi compito del Dirigente della UOB di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

5.8.3. Corrispondenza personale o riservata

La corrispondenza personale (es. Mario Rossi c/o nome Ente) è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale" o "s.p.m". In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale"o "s.p.m" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

5.8.4. Documenti inerenti a gare di appalto confezionati su supporti cartacei

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo" o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata alla UOB competente.

È compito della stessa UOB provvedere alla custodia delle buste o plichi protocollati, con mezzi idonei, sino all'espletamento della gara stessa, salvo diverse indicazioni che devono essere fornite all'Ufficio protocollo.

Dopo l'apertura delle buste la UOB che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti. Per motivi organizzativi tutte le UOB sono tenute ad informare preventivamente il Responsabile del Servizio archivistico in merito alle scadenze di concorsi, gare, bandi di ogni genere.

5.8.5. Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati. Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

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

5.8.6. Documenti pervenuti per errore all'Ente

I documenti pervenuti per errore all'Ente non devono essere protocollati e devono essere spediti immediatamente al destinatario con la dicitura «Erroneamente pervenuto all'E.R.S.U. Catania il ...».

5.8.7. Trattamento dei documenti con oggetto o smistamento plurimo

Ogni documento, anche se in più esemplari, deve essere individuato da un solo ed unico numero di protocollo, indipendentemente dal fatto che sia indirizzato, per competenza o per conoscenza, a una o più strutture amministrative e/o organi politici all'interno dell'Ente.

Di conseguenza, qualora pervenga un documento nel quale risultano evidenti più destinatari, l'addetto alla registrazione, prima di protocollarlo, deve verificare, attraverso il sistema informatico, che esso non sia già stato registrato dagli altri destinatari.

Qualora il documento sia già stato registrato si deve riportare la stessa segnatura anche sugli altri esemplari. Qualora la verifica sia impossibile, perché il documento è stato presentato a sportelli di registratura decentrati, e quindi protocollato con numeri diversi, il RPA avrà cura di creare i collegamenti opportuni.

Ai fini del calcolo dei tempi del procedimento amministrativo si tiene conto della data archivistica di quello protocollato per primo. Nel caso in cui, oltre alla pluralità di destinatari, il documento tratti anche una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e – conseguentemente – a fascicoli diversi, l'addetto alla registrazione deve individuare la classifica prevalente e smistare il documento acquisito a sistema alle UOB competenti indicando nel campo note "originale cartaceo alla UOB prima assegnataria" Ogni documento in uscita o interno deve obbligatoriamente trattare un solo oggetto (un solo argomento), deve necessariamente riferirsi ad un solo procedimento e quindi deve essere conservato in un unico fascicolo.

5.8.8. Documenti in partenza con più destinatari

Qualora i destinatari del documento siano molteplici nella registrazione di protocollo va selezionato dopo il primo nominativo se è trasmesso in nodo diretto o per conoscenza.

5.9. Regole di smistamento e di assegnazione

L'operazione di smistamento consiste nell'assegnazione di un documento registrato alla UOB competente e al conseguente conferimento di responsabilità del relativo procedimento amministrativo.

Si adottano le modalità operative di seguito illustrate:

➢ Tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia per immagine e associati alla registrazione di protocollo. Fanno eccezione i documenti che materialmente non possono essere sottoposti a scansione (a titolo meramente esemplificativo: volumi, registri, plichi, planimetrie di formato superiore all'A3, plastici, monete, ecc.). In questi casi si deve segnalare l'assenza degli allegati, nel campo "Annotazioni" del registro di protocollo, con la dicitura "Documento/i cartaceo/i";

➢ Nel caso di documento analogico, l'originale sarà conservato dal Responsabile del Procedimento;

➢ Nel caso di documenti informatici, l'originale sarà acquisito direttamente (salvo procedura di caricamento manuale) nel sistema di protocollo attraverso i canali previsti;

➢ É prevista una forma di assegnazione per conoscenza per i soli documenti a carattere conoscitivo privi di adempimenti per le UOB (come alcune circolari di contenuto informativo);

➢ Quotidianamente gli operatori e/o i responsabili aprono la scrivania di lavoro, attraverso la quale possono verificare i documenti pervenuti e monitorare i movimenti, precedenti o successivi degli stessi. Le scrivanie

di lavoro sono un valido strumento di gestione e di controllo sui documenti acquisiti, presi in carico o assegnati;

➢ Il responsabile dell'UOB visualizza i documenti, attraverso l'utilizzo di Easy Prot e in base alle abilitazioni previste potrà:

− Visualizzare gli estremi del documento

− Visualizzare il contenuto del documento

− Individuare come assegnatario il RPA competente sulla materia oggetto del documento;

➢ il RPA provvede alla visione e alla gestione del documento assegnato e mediante una delle seguenti azioni:

− Riassegnazione: assegnazione ad altro ufficio o ad utenti del proprio ufficio

− Rifiuto: restituzione del documento all'ufficio mittente in caso di errata assegnazione

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi e le modalità di gestione del flusso documentale ed i conseguenti riflessi sotto il profilo della responsabilità. La "presa in carico" dei documenti viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOB di competenza coincide con la data di assegnazione degli stessi.

6. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

6.1 Modalità di utilizzo del registro di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato Registro di emergenza.

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le due ore o che sia comunque tale da pregiudicare la registrazione a protocollo in giornata, nel caso in cui vi siano scadenze inderogabili e prescrittive (es: bandi, concorsi, ecc...).

L'utilizzo del registro di emergenza deve essere autorizzato dal RSP

Per la registrazione di emergenza si utilizza: 1. Nel caso di disponibilità dei PC un modulo in formato excel disponibile tra la modulistica presente in intranet; il modulo potrà essere compilato mediante l'immissione dei dati direttamente sulla tabella e dovrà essere successivamente salvato 2. Nel caso di impossibilità ad utilizzare i PC ci si avvarrà di un modulo che verrà compilato manualmente.

Sul registro di emergenza devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, la data e l'ora di ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico e della gestione documentale. Prima di autorizzare l'avvio della procedura, il RSP deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza.

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

L'UOB dovrà annotare nel protocollo informatico unico i periodi di attivazione del Registro di emergenza.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, UOB, anno di registrazione, numero di protocollo nel formato stabilito; ad esempio: E01-2015-Servizi Istituzionali e Avvocatura-0000005.

La segnatura del protocollo di emergenza deve essere apposta mediante timbro o altro dispositivo e riportare le informazioni desunte dal relativo registro.

Una volta ripristinata la piena funzionalità del sistema, il RSP provvede alla chiusura dei registri di emergenza; il sistema provvederà ad annotare su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura. I dati delle registrazioni di emergenza dovranno essere inseriti nel sistema informatico di protocollo e si configurano come un repertorio dello stesso.

Ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo senza soluzioni di continuità la numerazione del protocollo informatico unico raggiunta al momento dell'interruzione del servizio.

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

L'utente adibito alla protocollazione, alla ripresa della piena funzionalità del sistema di protocollo informatico, provvede a riversare sul programma stesso tutte le registrazioni già eseguite sul registro di emergenza. I documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

7. DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

7.1. Descrizione funzionale ed operativa

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo nel contesto organizzativo dell'Ente.

La struttura modulare, che risponde ad esigenze di organizzazione e razionalizzazione delle componenti del sistema, è stata concepita per essere in grado di affrontare successive implementazioni, aggiornamenti o modifiche senza comprometterne l'impianto di base e le funzionalità già realizzate. Il sistema consente di rappresentare informaticamente i meccanismi tipici dell'attività amministrativa nel contesto organizzativo dell'Ente riproducendo le principali azioni della gestione documentale. Ciò è possibile grazie a funzioni di amministrazione che consentono la gestione della struttura organizzativa (Organigramma), con i relativi ruoli operativi, definiti in base ai compiti assegnati agli utenti, ed a parallele funzioni di gestione delle scrivanie di lavoro virtuali a disposizione degli utenti.

Ai sensi della normativa vigente sono disponibili funzioni per la produzione delle registrazioni di protocollo e relative ricerche, stampe, statistiche e reportistica anche ai fini del controllo di gestione; funzioni per la produzione dei fascicoli informatici, del relativo repertorio e delle connesse funzionalità di ricerca; gestione dell'albo on-line e del registro delle pubblicazioni. Il sistema è integrato con tutti i canali di trasmissione

informatica dei documenti previsti dall'Ente (posta elettronica, posta certificata, interoperabilità, istanze on-line), dai quali i documenti informatici vengono acquisiti a protocollo.

7.2. Rilascio delle abilitazioni di accesso

Il presente paragrafo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso alle informazioni documentali gestite dal sistema di protocollo informatico e di gestione documentale Easy Prot.

Gli utenti del servizio di protocollo, in base agli uffici di appartenenza, ovvero in base alle rispettive competenze hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza.

Ad ogni utente è assegnata:

➢ una credenziale di accesso, costituita, ad esempio, da una componente:

− pubblica che permette l'identificazione dell'utente da parte del sistema (userID)

− privata o riservata di autenticazione (password)

➢ una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati agli utenti dal Responsabile della gestione documentale, che si avvale di un profilo di amministrazione.

Gli utenti del servizio di protocollo una volta identificati sono suddivisi in profili d'accesso, sulla base delle rispettive competenze.

La profilazione degli utenti nel sistema di protocollo informatico Easy Prot avviene mediante il modulo per la gestione dell'organigramma.

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli uffici e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono sottoposte a verifica, modifica, gestione e aggiornamento.

7.2.1. Abilitazioni interne ad accedere ai servizi di protocollo

Per accedere al programma di protocollo informatico e di gestione documentale è necessario essere registrati, cioè essere dotati di nome utente e password.

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato, la cui password non è accessibile.

7.2.2. Ripristino delle credenziali private d'accesso

In caso di smarrimento della password l'utente contatta l'amministratore del sistema e fa richiesta di una nuova password per accedere al sistema di protocollo.

7.2.3. Abilitazione alle registrazioni di protocollo riservato

L'utente del sistema può gestire (registrare, visualizzare, assegnare) documenti riservati solo se autorizzato tramite apposita abilitazione.

In fase di registrazione gli utenti autorizzati sono chiamati a definire il livello di riservatezza di un documento secondo quanto previsto dalle disposizioni legislative in materia di tutela dei dati personali e del diritto di accesso. Tale scelta incide conseguentemente sulla possibilità di visibilità e di gestione di un documento da parte di un utente, in base al livello di accesso assegnatogli.

I documenti registrati con tali forme appartengono al cosiddetto protocollo riservato, il cui accesso è autorizzato alle persone indicate da apposito regolamento, in relazione alle tipologie documentarie ed ai procedimenti amministrativi.

8. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

8.1. Protezione e conservazione degli archivi pubblici

8.1.1. Premessa

Ai sensi dell'art. 30 del D.lgs 42/2004, dell'art. 30 del Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, Norme relative all'ordinamento ed al personale degli archivi di Stato e degli artt. 67 e 69 del DPR 445/2000, l'Ente, in quanto ente pubblico, ha l'obbligo di:

➢ garantire la sicurezza e la conservazione del suo archivio e di procedere al suo ordinamento;

➢ costituire uno, o più archivi di deposito nei quali trasferire annualmente i fascicoli relativi agli affari conclusi;

➢ istituire una sezione separata d'archivio per i documenti relativi ad affari esauriti da più di 40 anni (archivio storico) e di redigerne l'inventario. L'archivio è quindi un'entità unitaria, che conosce però tre fasi: ➢ archivio corrente, composto dai documenti relativi ad affari in corso conservati presso gli uffici;

➢ archivio di deposito, composto dai documenti relativi ad affari cessati da meno di 40 anni conservati presso l'archivio di deposito di ogni UOB, oppure presso l'Archivio generale dell'Ente, a determinate condizioni;

➢ archivio storico, composto dai documenti relativi ad affari cessati da più di 40 anni, selezionati per la conservazione permanente conservati presso l'Archivio generale dell'Ente, che funge da sezione separata.

Il presente capitolo riporta il sistema di classificazione dei documenti, di formazione del fascicolo e di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario).

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

Il titolario e il piano di conservazione in quanto strumenti che consentono la corretta gestione e conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di registrazione di protocollo e di archiviazione. Spetta al Direttore adottare il titolario e il piano di conservazione con atti formali.

8.1.2. Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici sono beni culturali inalienabili ai sensi dell'art. 10, c. 2 del D.lgs 42/2004.

Quindi, tutti i documenti acquisiti e prodotti (compresi quelli interni) nel sistema di gestione documentale dell'Ente sono inalienabili e appartengono ad un unico complesso archivistico, che è l'archivio dell'Ente.

L'archivio non può essere smembrato e deve essere conservato nella sua organicità. Lo scarto dei documenti, siano essi cartacei o informatici, è subordinato all'autorizzazione della Soprintendenza archivistica della Regione ai sensi degli artt. 20 e 21 del D.lgs 42/2004.

L'Ente adotta le misure previste dal D.Lgs 196/2003 e ss.mm.ii. a tutela delle informazioni, dei dati e dei documenti.

8.2. Titolario o piano di classificazione

8.2.1. Titolario

Il Titolario o Piano di classificazione è un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti.

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

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

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione. L'Ente utilizza il Titolario di classificazione elaborato da Easy Prot per la formulazione di proposte e modelli per la riorganizzazione dell'archivio.

Il titolario può essere aggiornato e le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente, previa informazione a tutti i soggetti abilitati all'operazione di classificazione dei documenti.

8.2.2. Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo l'ordinamento del titolario.

Viene effettuata su tutti i documenti ricevuti e prodotti dalle UOB dall'Ente, indipendentemente dal supporto sul quale vengono formati. La classificazione (apposizione/associazione di titolo, classe, sottoclasse, al documento) è necessaria e preliminare all'attività di fascicolazione.

8.3. Fascicolazione

8.3.1. Fascicolazione dei documenti

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

Il sistema informatico genera e aggiorna automaticamente il repertorio dei fascicoli all'apertura di un nuovo fascicolo.

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

TIPOLOGIE DI FASCICOLO

Si distinguono due tipologie di fascicolo:

➢ Fascicoli relativi ad affari o procedimenti amministrativi

➢ Fascicoli relativi a persone fisiche o giuridiche (ad esempio: personali dipendente, assistiti, associazioni, attività economiche, etc.)

Fascicoli relativi ad affari o procedimenti amministrativi

Qualora un documento dia luogo all'avvio di un autonomo affare o procedimento amministrativo, il RPA assegnatario del documento stesso deve provvedere all'apertura (istruzione) di un nuovo fascicolo e comprende la registrazione di alcune informazioni essenziali:

➢ anno

➢ indice di classificazione, (cioè titolo, classe, sottoclasse, etc.)

➢ numero del fascicolo

➢ oggetto del fascicolo

➢ data di apertura del fascicolo

➢ AOO e UOB

➢ nominativo del responsabile Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario.

Il RPA provvede anche all'archiviazione dei documenti all'interno del fascicolo.

I documenti sono archiviati all'interno di ciascun fascicolo, secondo l'ordine cronologico di registrazione, in base cioè al numero di protocollo ad essi attribuito. Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare.

La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Esso va archiviato rispettando l'ordine del repertorio, vale a dire l'anno di apertura.

Fascicoli relativi a persone fisiche o giuridiche

Per ogni persona fisica o giuridica deve essere istruito un fascicolo nominativo. Il fascicolo viene aperto al momento dell'inizio del rapporto con l'Ente e viene chiuso al momento della cessazione del rapporto. L'apertura prevede la registrazione di alcune informazioni essenziali:

➢ anno

➢ indice di classificazione, (cioè titolo, classe, sottoclasse, etc.)

➢ indicazione della serie e del numero identificativo del fascicolo al suo interno

➢ oggetto del fascicolo

➢ data di apertura del fascicolo

➢ AOO e UOB

➢ nominativo del responsabile

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario.

All'interno di ciascuna serie i fascicoli vanno conservati nell'ordine prestabilito secondo criteri che rispondano ad opportunità ed efficacia (es. ordine cronologico di instaurazione del rapporto, ordine alfabetico, ...).

8.3.2. Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'amministrazione, l'UOB abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un fascicolo già esistente, oppure sia necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

➢ Se il documento si ricollega ad un fascicolo aperto, l'addetto: − seleziona il relativo fascicolo − collega la registrazione di protocollo del documento al fascicolo selezionato (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo)

➢ Se il documento non è collegabile ad alcun fascicolo aperto, il soggetto preposto: − esegue l'operazione di apertura del fascicolo − collega la registrazione di protocollo del documento al nuovo fascicolo aperto

8.3.3. Repertorio dei fascicoli

Lo strumento di gestione e organizzazione dei fascicoli è il Repertorio dei fascicoli, i cui elementi costitutivi sono:

➢ l'anno di riferimento

➢ l'indice di classificazione completo (titolo, classe, sottoclasse, etc.)

➢ il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli e inserti)

➢ la data/anno di apertura

➢ la data/anno di chiusura

➢ l'oggetto del fascicolo

➢ l'annotazione sullo stato del fascicolo, cioè se è aperto o chiuso

➢ eventuali annotazioni

8.4. Serie archivistiche e repertori

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono. Ai fini del loro facile reperimento, alcuni documenti, come i verbali, le deliberazioni degli organi di governo dell'amministrazione o i contratti, sono soggetti a registrazione particolare (repertorio).

I documenti repertoriati costituiscono una serie archivistica; possono essere altresì conservati in un fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Lo strumento fondamentale per l'individuazione delle serie e dei repertori nell'Ente è il Titolario di classificazione.

9. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

9.1. Premessa

L'Ente, recependo le prescrizioni e i principi espressi dalla normativa in materia, ha disciplinato le attività e i procedimenti amministrativi definendo le responsabilità in ordine agli stessi. Attraverso appositi regolamenti garantisce da un lato l'accesso il più ampio possibile ai documenti amministrativi e dall'altro la tutela dei dati personali e sensibili, riconoscendo in tal modo diritti entrambi costituzionalmente fondati.

Al fine di assolvere agli obblighi di pubblicità legale ai sensi della legge 18 giugno 2009, n. 69, l'Ente ha attivato un sistema di gestione dell'Albo on-line integrato nel sistema di protocollo e gestione documentale Easy Prot e conforme ai requisiti previsti, e ha regolamentato le modalità, le forme e i limiti con i quali deve essere organizzato e gestito.

In adempimento alla recente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013) l'Ente ha costituito apposita sezione di "Amministrazione trasparente" nel sito istituzionale, nella quale sono pubblicati dati, informazioni e documenti che riguardano l'organizzazione e le attività dell'amministrazione. Attraverso apposita sottosezione di Amministrazione trasparente è possibile consultare l'elenco dei procedimenti amministrativi dell'Ente attraverso funzionalità di ricerca per settore o

per argomento. Nelle forme previste dalla normativa (art. 10 del citato D. lgs. 33/2013) pubblica ed aggiorna annualmente il Programma triennale per la trasparenza e l'integrità ed il relativo stato di attuazione.

9.2. Procedure di accesso ai documenti e di tutela della riservatezza

Merita chiarire preliminarmente alcuni principi e procedure che costituiscono un punto di riferimento per chi opera nell'Ente, tenendo conto che le problematiche connesse all'accesso e alla tutela della riservatezza riguardano tutte le fasi di vita dei documenti.

L'accesso/consultazione dei documenti si può così suddividere: 1. Consultazione per fini amministrativi, per la quale si fa riferimento allo specifico regolamento comunale già citato, che può riguardare tutta la documentazione prodotta dall'Ente nell'esercizio della sua attività amministrativa, ivi compresa quella conservata nell'archivio storico. 2. Consultazione per fini di ricerca storico-scientifica, che è disciplinata dal Capo III del Codice dei Beni Culturali e del Paesaggio, in base al quale i documenti dell'Ente sono liberamente consultabili, ad eccezione: − di quelli di carattere riservato relativi alla politica estera o interna dello Stato, che divengono consultabili 50 anni dopo la chiusura del fascicolo che li contiene − di quelli contenenti dati sensibili, che diventano consultabili 40 anni dopo la chiusura del fascicolo che li contiene − di quelli contenenti taluni dati sensibili (noti in gergo come "sensibilissimi"), idonei a rivelare lo stato di salute o la vita sessuale o i rapporti riservati di tipo familiare, che diventano consultabili 70 anni dopo la chiusura del fascicolo che li contiene.

La consultazione dei documenti contenenti dati sensibili può essere autorizzata dalla Soprintendenza archivistica competente per territorio anche prima della scadenza dei termini prescritti dalla legge.

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

10.1. Modalità di approvazione e aggiornamento del Manuale

Il presente Manuale è approvato dall' Ente con propria deliberazione ed è aggiornato con le medesime modalità. Gli aggiornamenti potranno rendersi necessari a seguito di: ➢ adeguamenti normativi che rendano superate le prassi definite nel Manuale ➢ introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza ➢ inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Gli allegati al presente Manuale, che contengono indicazioni di dettaglio sulle procedure operative e sulle modalità di funzionamento dei sistemi gestionali, sono modificati con Decreti del Direttore

Entra in vigore alla data di esecutività della deliberazione che lo approva.

10.2. Pubblicità del presente Manuale

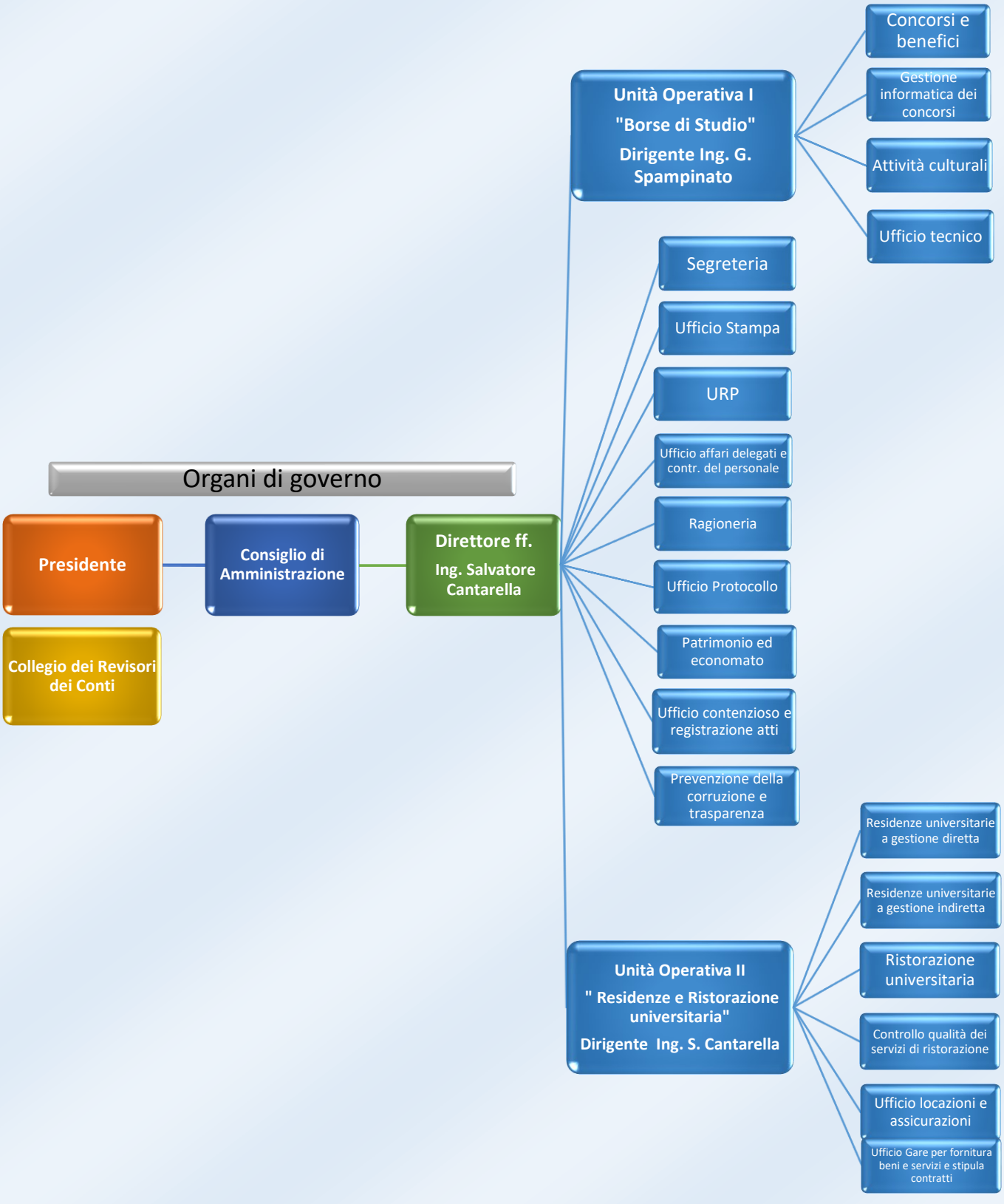
In ottemperanza a quanto disposto dal comma 3 dell'art. 5 del DPCM 3 dicembre 2013, il Manuale di gestione è reso pubblico dall'Ente mediante la pubblicazione sul proprio sito istituzionale.

Regione Siciliana
E. R. S. U
Università degli Studi
Catania

ORGANIGRAMMA E.R.S.U DI CATANIA

Ai sensi del D.D.G. n. 756/Dir del 28/11/2001 dell'Ass.to Reg.le dei BB.CC.AA. e P.I. – Dip. Reg.le Istruzione

e successivi contratti dirigenziali individuali



Gestione Titolario

(/protocol/settings)

+ (/protocol/filing_plans/new)

Titolo	Nome	Creato il	Classi	Codice Interno	
1	**Protocollo Informatico**	08 Set 18:34	0		(/protocol/filing_plans/557/edit)
2	**Albo Fornitori**	08 Set 18:34	0		(/protocol/filing_plans/558/edit)
3	**Gestione Documentale**	16 Gen 11:53	0		(/protocol/filing_plans/559/edit)
3	**Gestione Gare**	16 Gen 11:53	0		(/protocol/filing_plans/696/edit)

Precedente 1 Successivo