

# **Regolamento per la gestione, la tenuta e la tutela dei documenti amministrativi dal protocollo all'archivio storico**

## DOCUMENTAZIONE AMMINISTRATIVA

### **Documento informatico**

Il T.U. 445/2000 stabilisce che il documento informatico da chiunque formato, la sua registrazione su supporto informatico e la sua trasmissione mediante strumenti telematici hanno piena rilevanza giuridica a tutti gli effetti di legge.

Il decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513* stabilisce:

- le regole tecniche, per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, (o cifratura di messaggi) anche solo temporanea, dei documenti informatici; tali regole, ogni due anni, saranno adeguate all'evoluzione scientifica e tecnologica;
- le misure tecniche, organizzative e gestionali che garantiscono l'integrità, la disponibilità e la riservatezza dei dati contenuti nel documento informatico con riferimento al possibile uso di chiavi biometriche.

Anche per il documento informatico rimangono valide le disposizioni riguardanti, la tutela dei dati personali.

### **Documenti informatici delle aziende sanitarie e ospedaliere italiane.**

I documenti e i dati informatici come pure gli atti formati con strumenti informatici sono da considerarsi a tutti gli effetti originali e fonte primaria di notizia. Da questi, su diversi tipi di supporto, è possibile riprodurre copie per gli usi consentiti dalla legge.

In tutte le operazioni informatiche che riguardano la produzione, l'immissione, la conservazione, la riproduzione, l'emanazione di atti e la trasmissione di dati, documenti e atti amministrativi con sistemi informatici e telematici, si devono indicare e rendere facilmente individuabili sia i dati relativi alle amministrazioni interessate sia il soggetto che ha effettuato l'operazione.

La Deliberazione AIPA del 23 novembre 2000 n. 51 *Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513* disciplina, d'intesa con il Ministero per i beni e le attività culturali, le regole tecniche per la formazione e la conservazione dei documenti informatici; per il materiale classificato le regole sono stabilite d'intesa con il Ministero della difesa, dell'interno e delle finanze.

### **Forma e validità del documento informatico art. 10 da rivedere.**

Il documento informatico risponde al requisito della forma scritta e ha efficacia probatoria ai sensi dell'art. 2712 del C.C. (*Riproduzioni meccaniche*) quando:

- è sottoscritto con firma digitale; la firma digitale conferisce al documento anche la validità di scrittura privata ai sensi dell'art. 2702 del C.C. (*Efficacia della scrittura privata*)
- è redatto conformemente alle regole tecniche stabilite dal decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999,

- è redatto in conformità alle regole stabilite dall'AIPA, d'intesa con il Ministero per i beni e le attività culturali – Deliberazione n. 51/2000

Tutti i documenti fiscali (o contabili) informatici, purchè redatti in conformità alle regole tecniche stabilite dal D.P.C.M. 8 febbraio 1999, rispondono ai requisiti previsti dagli articoli 2214 e seguenti del C.C. e da ogni altra disposizione legislativa o regolamentare ( art. 2214 – *Libri obbligatori e altre scritture contabili*; art. 2215 – *Libro giornale e libro degli inventari*; art. 2216 – *Contenuto del libro giornale*; art. 2217 – *Redazione dell'inventario*; art. 2218 – *Bollatura facoltativa*; art. 2219 – *Tenuta della contabilità*; art. 2220 – *Conservazione delle scritture contabili*; art. 2221 – *Fallimento e concordato preventivo*)

Il decreto del Ministero delle Finanze definisce le regole, con le quali sono assolti gli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione.

### **Stipulazione di contratti con strumenti informatici o per via telematica.**

I contratti che le aziende stipulano con strumenti informatici oppure per via telematica, e per i quali si applicano le disposizioni vigenti sui contratti negoziati fuori dei locali commerciali, sono validi a tutti gli effetti di legge.

### **Trasmissione del documento informatico.**

Il documento informatico, conforme alle disposizioni del T.U. 445/2000, alle regole tecniche di cui al DPCM 8 febbraio 1999 e alla Deliberazione AIPA 51/2000, s'intende inviato o pervenuto per via telematica, se il mittente lo trasmette all'indirizzo elettronico che il destinatario ha reso pubblico. L'avvenuta ricezione del destinatario è da considerarsi una presunzione iuris tantum. La prova esibita dal mittente, opponibile ai terzi, risulta dalla validazione temporale del documento informatico: data e ora di formazione e trasmissione del documento informatico. (masucci pag 43)

Il documento informatico è di proprietà del mittente fin quando il gestore del sistema di trasporto non lo consegna al destinatario.

La notifica telematica di un documento informatico ha lo stesso valore giuridico della notificazione che avviene tramite posta. Il mittente deve comunque dare prova dell'inoltro e della consegna del documento, La certificazione dell'avvenuta consegna è disciplinata dalla Circolare 7 maggio 2001, n. AIPA/CR/28 – punto 6 – 6.1. Il messaggio di conferma di ricezione, richiesto dall'AOO mittente e indicata nella segnatura informatica del messaggio, ha lo scopo di certificare l'avvenuta protocollazione in ingresso del messaggio ricevuto.

### **Segretezza del documento trasmesso per via telematica.**

L'operatore addetto alla trasmissione del documento informatico non può:

- prendere visione del documento,
- duplicare il documento con qualunque mezzo,
- cedere il documento a terzi a qualsiasi titolo anche se per estratto e in forma sintetica, salvo che le informazioni per loro natura o per indicazione del mittente possono essere pubbliche.

### **Copie di atti e documenti informatici.**

Il documento informatico - copia, estratto e duplicato - che riproduce e rappresenta letteralmente e integralmente altro documento informatico o un documento cartaceo è valido a tutti gli effetti di legge se conforme alle disposizioni del T.U. 445/2000.

La firma digitale dell'interessato (apposta o associata al documento informatico) attribuisce piena efficacia giuridica al documento informatico contenente la copia o la riproduzione di atti pubblici, di scritture private e di atti e documenti amministrativi inviati o spediti da soggetti pubblici autorizzati o da pubblici ufficiali (art. 2714 C.C. – *Copie di atti pubblici*; art. 2715 C.C. – *Copie di scritture private depositate*).

La firma digitale garantisce pertanto l'integrità e la fedeltà di quanto contenuto nel documento informatico che sostituisce a tutti gli effetti, il documento cartaceo.

Il notaio o altro pubblico ufficiale autorizzato attesta, con dichiarazione allegata al documento informatico e rispondente alle regole del DPCM 8 febbraio 1999, che le copie informatiche di documenti originariamente cartacei o in ogni caso non informatici sostituiscono ad ogni effetto di legge i loro originali.

Le copie digitali di atti e documenti con firma digitale dell'interessato possono essere prodotte ed esibite al posto dell'originale cartaceo.(Masucci)

Il documento informatico soddisfa tutti gli effetti di legge e agli obblighi di conservazione e di esibizione se le procedure seguite sono quelle previste dalle regole tecniche del DPCM 8 febbraio 1999.

## DEFINIZIONI

**Atto amministrativo:** *tutti gli atti unilaterali aventi rilevanza esterna posti in essere da una Pubblica Amministrazione nell'applicazione di una potestà amministrativa.*

**Copia:** riproduzione e rappresentazione fedele e integrale di un documento.

**Copia digitale:** documento informatico che riproduce e rappresenta un documento cartaceo o informatico.

**Documentazione:** manifestazione di volontà di un soggetto per creare un documento.

**Documento amministrativo informatico:** rappresentazione informatica di fatti o atti giuridicamente rilevanti, di provvedimenti amministrativi, di atti interni della pubblica amministrazione, di atti di diritto privato della pubblica amministrazione finalizzati ad interessi pubblici e di atti formati da un privato e utilizzati per fini amministrativi.

**Documento amministrativo:** rappresentazione, comunque formata, del contenuto di atti, anche interni delle pubbliche amministrazioni o comunque usati ai fini dell'attività amministrativa.

**Documento elettronico:** documento formato mediante un sistema elettronico. masucci pag 16 nota

**Documento sanitario:** documento prodotto o acquisito da un'Azienda sanitaria o ospedaliera nello svolgimento delle proprie attività istituzionali: amministrativa e sanitaria.

**Documento:** rappresentazione giuridica di un fatto o atto che permane nel tempo.

**Duplicato:** documento che riproduce altro documento, rappresentativo dell'atto (pag 48 nota masucci)

**Estratto:** riproduzione parziale e puntuale di un documento.

**Fatto e atto giuridico.** Fatto: eventi cui la norma giuridica collega conseguenze giuridiche; atto giuridico: fatti giuridici che consistono in comportamenti volontari delle persone.

Non è un documento informatico quello prodotto con sistemi informatici mediante procedimenti di stampa su carta.

**Provvedimento amministrativo:** *atti autoritativi tipici e nominati preordinati alla realizzazione di interessi specifici dell'amministrazione e consistenti in statuizioni destinate a produrre modificazioni eventualmente richieste dagli interessati o quelle che l'amministrazione sia ex officio tenuta a decidere se operare o meno a certe scadenze fisse o in certe situazioni indicate dalla legge.*

## FIRMA DIGITALE

### Atti preliminari alla formazione della firma digitale

Per la formazione della firma digitale occorre:

1. registrare l'utente presso un'Autorità di Certificazione (la P.A. può svolgere attività di certificazione e pertanto deve iscriversi nell'elenco pubblico dei certificatori tenuto e aggiornato dall'AIPA nel rispetto delle regole tecniche del DPCM 8 febbraio 1999 e delle disposizioni contenute nella Circolare 16 febbraio 2001, n. AIPA/CR/27.
2. Generare una coppia di chiavi.
3. Certificare la chiave pubblica.
4. Registrare la chiave pubblica.

### Processo di apposizione della firma digitale

Tale processo prevede tre fasi:

1. Generazione dell'impronta. Si effettua applicando una funzione hash che oltre a produrre una sequenza di numeri binari la cui lunghezza minima è stabilita in 1024 bit, garantisce l'unicità della sequenza stessa.
2. Generazione della firma digitale attraverso la cifratura dell'impronta.
3. Apposizione della firma digitale sul documento

### Firma digitale: natura giuridica e caratteristiche

La firma digitale, apposta su un documento informatico, su un gruppo di documenti, duplicati o copie, è l'**esito** di una procedura informatica che sostituisce a tutti gli effetti, la firma autografa con la quale si sottoscrive un documento cartaceo. Può essere trasmessa direttamente con il documento oppure separatamente purché sia sempre ad esso associato.

La firma digitale come la firma autografa deve riferirsi in modo univoco ad una persona fisica, a un documento o a un gruppo di documenti. E' pertanto uno strumento in grado di assicurare:

- la provenienza del documento informatico (autenticità, veridicità e attendibilità);
- l'integrità del documento informatico (mancanza di modificazioni);
- la probatorietà del documento informatico (validità giuridica del contenuto);
- la non ripudiabilità del documento informatico (il soggetto che ha inviato il documento informatico non può negare, in un momento successivo, di averlo fatto);

Essa si basa su un sistema di chiavi a coppia e asimmetriche (**codici informatici composti da algoritmi**) che consentono di cifrare, decifrare e validare il documento. Il sistema asimmetrico assicura una maggiore sicurezza al sistema in quanto la conoscenza della chiave pubblica non fornisce alcuna informazione sulla chiave privata.

La sicurezza del sistema di cifratura è di tipo computazionale (per le normali capacità di calcolo del computer, è difficilissimo entrare nel meccanismo della cifratura)

Le chiavi componenti la coppia, una pubblica e una privata, sono strettamente correlate. Ciò significa che, un documento cifrato con una delle due chiavi può essere decifrato solo dall'altra e la firma apposta o associata con una chiave (privata) può essere verificata solo dall'altra (pubblica). Tale chiave, certificata da un'apposita autorità di certificazione, non deve essere scaduta, revocata o sospesa.

La firma digitale apposta su un documento integra e sostituisce l'apposizione di punzoni, sigilli, timbri, contrassegni e marchi di qualunque tipo.

Il DPCM 8 febbraio 1999 stabilisce come attraverso la firma digitale si possono individuare gli elementi che consentono di identificare il soggetto titolare della firma, l'autorità di certificazione e il registro su cui è pubblicata per la consultazione.

### Revoca e sospensione della firma digitale

La revoca o la sospensione, motivate, hanno effetto dalla pubblicazione a meno che il revocante o colui che chiede la sospensione non dimostri che tutti gli interessati n'erano a conoscenza.

La firma digitale apposta o associata con chiave revocata o sospesa ha lo stesso valore della mancata sottoscrizione.

### **Firma digitale autenticata**

Ai sensi dell'art. 2703 del C.C. (*Sottoscrizione autenticata*), si ha per riconosciuta la firma digitale la cui apposizione è autenticata da notaio, o da altro pubblico ufficiale autorizzato. Pertanto la firma digitale autenticata ha gli stessi effetti della firma autografa autenticata.

Il pubblico ufficiale, che previamente accerta l'identità personale del firmatario, attesta:

- che il titolare ha apposto la firma digitale in sua presenza;
- la validità della chiave utilizzata;
- la volontà del titolare a sottoscrivere l'atto
- che il documento sottoscritto sia conforme all'ordinamento giuridico – art. 28, primo comma, n. 1 della legge n. 89 del 6 febbraio 1913.

La firma digitale del pubblico ufficiale integra e sostituisce ad ogni effetto di legge sigilli, punzoni, timbri, contrassegni e marchi di ogni tipo.

Il pubblico ufficiale può allegare al documento informatico copia informatica autenticata di documenti formati su supporti diversi come indicato in documentazione Amministrativa . copie di atti e documenti informatici – punto 4.

La firma digitale si intende apposta dinanzi a pubblico ufficiale se inserita nel documento informatico o depositato o esibito presso una pubblica amministrazione.

Il documento informatico, presentato o depositato presso una pubblica amministrazione per via telematica, è valido se munito di firma digitale e se indica data e ora della sottoscrizione.

### **Firma dei documenti informatici delle pubbliche amministrazioni**

La firma autografa apposta sui documenti di una pubblica amministrazione è sostituita dalla firma digitale.

Essa sostituisce e integra l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi.

**La firma digitale, dando validità giuridica al documento informatico, non sana eventuali vizi di volontà che inficiano l'atto.**

### **Deposito della chiave privata**

Il soggetto titolare della coppia di chiavi asimmetriche, per assicurarsi sempre una copia della chiave o per dimostrare in un qualunque momento di esserne il legittimo proprietario e quindi il sottoscrittore, può depositare, in forma segreta, la chiave privata presso un notaio o altro pubblico ufficiale. Il depositario non può in alcun modo utilizzarla né per interessi personali né per altri fini.

Il titolare può, a sua cura, registrare la chiave su qualunque tipo di supporto e consegnarla in un involucro sigillato al notaio o ad altro pubblico ufficiale; tanto per evitare che il contenuto sia letto, conosciuto o estrapolato mediante rotture o alterazioni.

Tale procedura garantisce la segretezza della chiave privata.

L'art. 605 C.C. *Formalità del testamento segreto* disciplina il deposito della chiave privata è la stessa del testamento segreto –.

### **Certificazione delle chiavi**

Chiunque intenda redigere un documento informatico, registrarlo su un supporto informatico oppure trasmetterlo per via telematica, deve munirsi della coppia di chiavi asimmetriche e rendere pubblica una di esse attraverso la procedura della certificazione (DPCM 8 febbraio 1999 e Circolare 16 febbraio 2001 AIPA/CR/27).

La certificazione è un processo informatico mediante il quale si attestano sia la corrispondenza tra soggetto titolare e chiave pubblica sia il periodo di validità della chiave. Le attività di certificazione possono essere svolte da soggetti pubblici o privati.

I certificatori privati, mediante un'apposita dichiarazione antecedente all'inizio dell'attività, sono inclusi in un elenco pubblico predisposto, tenuto e aggiornato dall'AIPA e consultabile via telematica.

Il certificatore per l'importante ruolo che svolge deve possedere i seguenti requisiti:

- deve trattarsi di una S.p.A. con capitale sociale non inferiore a quello previsto per l'autorizzazione all'attività bancaria;
- i legali rappresentanti e i soggetti preposti all'amministrazione devono possedere i requisiti dell'onorabilità ;
- i rappresentanti tecnici e il personale addetto alla certificazione, per competenza ed esperienza professionale, sono in grado di osservare le norme del T.U. 445/2000 e le regole tecniche contenute nel DPCM 8 febbraio 1999.
- la certificazione di qualità dei servizi informativi su standard internazionali.

Il certificatore può operare, avendo sempre gli stessi requisiti, anche su licenza o autorizzazione rilasciata da uno Stato dell'U.E. o dello Spazio economico europeo.

Il certificatore custodisce le chiavi per un periodo non inferiore a dieci anni e dal momento della loro valutabilità, a sua cura, sono consultabili, via INTERNET.

### **Obblighi dell'utente e del certificatore**

Sia l'utente sia il certificatore, che intendono utilizzare il sistema di chiavi asimmetriche o la firma digitale, **ha il dovere di adottare** misure organizzative e tecniche tali da evitare danni ad altri.

Le funzioni del certificatore riguardano:

1. l'attività di identificazione;
2. l'attività di certificazione;
3. l'attività di pubblicazione delle chiavi pubbliche e gestione degli archivi;
4. l'attività di attestazione della validità del certificato mediante la pubblicazione e l'aggiornamento degli elenchi dei certificati sospesi e revocati;
5. l'attività di informazione e comunicazione
6. altro

#### Attività di identificazione.

Il certificatore identifica il titolare della chiave; la persona che fa richiesta della certificazione, specifica, con l'assenso del terzo interessato e su richiesta dell'istante, la presenza di poteri di rappresentanza o di altri titoli inerenti l'attività o altre cariche rivestite (il direttore generale, titolare di una chiave pubblica, è autorizzato a firmare con firma digitale perchè rappresentante legale dell'azienda sanitaria o ospedaliera. Ciò non preclude che il direttore generale, a titolo personale, possa essere titolare di altra coppia di chiavi).

### Attività di certificazione

Il certificatore esegue la certificazione e rilascia il certificato, documento informatico avente i requisiti stabiliti dal DPCM 8 febbraio 1999, che attesta il collegamento tra il titolare della chiave pubblica e la stessa chiave.

### Attività di pubblicazione delle chiavi pubbliche e gestione degli archivi

IL certificatore pubblica il certificato e la chiave pubblica che diviene consultabile via telematica. Provvede anche a pubblicare con immediatezza la revoca o la sospensione di chiavi asimmetriche. Altra funzione del certificatore riguarda una corretta gestione degli archivi, di cui deve garantire la continua consultabilità.

### Attività di attestazione della validità del certificato mediante la pubblicazione e l'aggiornamento degli elenchi dei certificati sospesi e revocati

Il certificatore attesta inoltre la validità del certificato e procede, con tempestività, all'aggiornamento dei certificati sospesi o revocati. Un certificato è sospeso se il certificatore ne sospende la validità per un determinato periodo di tempo; è revocato se ne annulla la validità. Ciò avviene nel caso che il titolare della chiave non intenda più utilizzarla e quindi chiede la revoca, oppure in caso di perdita del possesso della chiave, per un provvedimento dell'autorità, o perché il certificatore è venuto a conoscenza di cause che limitano la capacità del titolare per abusi o falsificazioni.

### Attività di informazione e comunicazione

Il certificatore ha la responsabilità di informare in modo chiaro i richiedenti sulla procedura di certificazione e sui requisiti tecnici per potervi accedere; deve inoltre comunicare con immediatezza all'AIPA e agli utenti, con preavviso di almeno sei mesi, la cessazione della propria attività e la rilevazione della documentazione da parte di altro certificatore o del suo annullamento.

### Altro

Il certificatore non può essere depositario della chiave privata; ciò evita che possa apporre la firma digitale del titolare.

Deve, altresì attenersi alle regole di cui al DPCM 8 febbraio 1999 e alle misure minime di sicurezza per il trattamento dei dati personali, emanate ai sensi dell'art. 15, comma 2 della legge 675/1996 ( D.P.R. 318/1999)

### **Chiavi di cifratura della pubblica amministrazione**

Le aziende sanitarie e ospedaliere, tenendo conto del proprio ordinamento, provvedono in modo autonomo alla generazione, alla conservazione, alla certificazione e all'utilizzo delle chiavi pubbliche.

Il DPCM 8 febbraio 1999 al Titolo IV art. 62 (*Certificazione da parte delle Pubbliche Amministrazioni*) stabilisce le modalità di formazione, di pubblicità, di conservazione, di certificazione e utilizzo delle chiavi pubbliche.

Il Ministro della giustizia o un suo delegato certifica e pubblica le chiavi pubbliche di ordini e albi professionali legalmente riconosciuti e dei loro rappresentanti.

Le chiavi pubbliche di pubblici ufficiali, non dipendenti di pubbliche amministrazioni, sono certificate e pubblicate in modo autonomo nel rispetto delle disposizioni vigenti, legislative e regolamentari, in materia di firme autografe nell'ambito dei rispettivi ordinamenti giuridici.

RIGUARDARE

## DEFINIZIONI

**Firma digitale:** è il risultato della procedura informatica (validazione) basata su uno schema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite una 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 .D.P.R. 445/2000

**Certificazione:** attestazione informatica, che non può essere superiore a tre anni, risultante da una procedura informatica, relativa alla chiave pubblica e rilevabile dai sistemi di validazione che prova:

**Chiave (codice) biometrica:** successione di codici informatici che nell'ambito di un sistema di sicurezza verificano l'identità personale dell'utente su sue specifiche caratteristiche fisiche.

**Chiave (codice) privata:** elemento della coppia di chiavi asimmetriche conosciuto solo dal proprietario; essa consente l'apposizione della firma digitale e decifra il documento informatico precedentemente formulato attraverso la corrispondente chiave pubblica.

**Chiave (codice) pubblica:** chiave asimmetrica pubblica; permette di verificare la firma digitale del titolare della chiave privata che ha redatto il documento informatico e di cifrare il documento informatico da trasmettere al titolare.

**Chiavi (codici) asimmetriche:** due chiavi crittografiche, una pubblica e una privata, strettamente collegate tra loro in modo tale che un documento cifrato da una chiave può essere decifrato solo con l'altra chiave alla prima collegata.

**Digitale:** risultato di calcoli numerici

- il periodo di validità della chiave che non può superare i tre anni.
- l'identificazione del soggetto titolare della chiave pubblica,
- la corrispondenza biunivoca tra il soggetto titolare della chiave pubblica e la persona fisica che la utilizza

**Validazione temporale:** attribuzione informatica di data e ora al documento (informatico)

**Sistema di validazione:** procedura informatica e crittografica che consente la generazione, l'apposizione e la verifica della validità della firma digitale.

## **GESTIONE INFORMATICA DEI DOCUMENTI**

( N:B:il paragrafo dove compare la sigla MG significa che quanto scritto è valido anche per la redazione del manuale di gestione)

### **Attuazione dei sistemi - MG**

Entro il 31 dicembre 2003 le AA.SS. e OO. Devono progettare o rimodulare i progetti inerenti i propri sistemi informativi e introdurre il protocollo informatico in conformità alle disposizioni del T.U. 445/2000 e alle disposizioni in materia di tutela dei dati personali. Pertanto i registri di protocollo cartacei saranno sostituiti da quelli informatici.

Nell'ambito della propria organizzazione le aziende dovranno individuare le aree organizzative omogenee e assicurare criteri uniformi finalizzati a una corretta comunicazione interna e alla classificazione e archiviazione dei documenti.

### **Sviluppo dei sistemi informativi - MG**

Lo sviluppo dei sistemi informativi aziendali deve avvalersi delle disposizioni del T.U. 445/2000 e delle norme tecniche stabilite dall'AIPA.

Le aziende sanitarie e ospedaliere, in attuazione al T.U. 445/2000 e alle norme sulla riservatezza dei dati personali, devono attuare o revisionare i propri sistemi informativi al fine di automatizzare le fasi di produzione, gestione, diffusione e utilizzazione dei propri dati, documenti, procedimenti e atti.

Inoltre dovranno valutare, secondo un rapporto di costi benefici, la possibilità di riportare su un supporto informatico tutta la documentazione cartacea di cui è necessaria la conservazione e predisporranno per la sostituzione di archivi cartacei con archivi informatici.

### **Il sistema di gestione informatica dei documenti: atti preliminari- MG**

Perché un sistema di gestione informatica dei documenti funzioni, è necessario definire preliminarmente i seguenti elementi:

1. individuazione e definizione di un o più aree organizzative omogenee. Per AOO si intende una struttura dotata di autonomia organizzativa e di spesa cui confluiscono uguali tematiche per le quali è possibile una gestione documentale omogenea e coordinata.
2. Individuazione e definizione dell'ufficio "utente". L'ufficio utente di un' AOO utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
3. Individuazione del Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi. Un dirigente o un funzionario, con adeguati requisiti professionali, avranno il compito di gestire il protocollo informatico, i flussi documentali e gli archivi.
4. Il responsabile del protocollo informatico dovrà essere unico anche in presenza di più aree organizzative omogenee. Ogni azienda, comunque, potrà decidere in piena autonomia.
5. Introduzione del protocollo unico. Con l'introduzione del protocollo unico cessano di fatto e di diritto ogni altra forma di registrazione dei documenti.
6. Adozione del titolario di classificazione. Il titolario di classificazione è uno strumento che consente un'organizzazione logica e organica dei documenti.
7. Massimario di selezione e scarto dei documenti. Il massimario è uno strumento che consente di verificare il tempo di conservazione di un documento cartaceo o informatico.

### **Il sistema di gestione informatica dei documenti MG**

1. Il sistema di gestione informatica dei documenti deve:
2. assicurare la sicurezza e l'integrità del sistema;
3. garantire la registrazione di protocollo dei documenti in entrata e in uscita in modo corretto e puntuale;
4. garantire una corretta gestione archivistica del documento (Titolario di classificazione e massimario di selezione e scarto);
5. fornire il collegamento tra il documento ricevuto e i documenti formati dall'azienda nell'adozione di provvedimenti finali;
6. consentire la ricerca facile e con più motori di ricerca, dei documenti protocollati;
7. consentire l'accesso al proprio archivio a soggetti interni ed esterni nel rispetto delle disposizioni in materia di tutela dei dati personali L. 675/1996 e successive modifiche e integrazioni.

### **Registrazione di protocollo MG**

Sono soggetti alla registrazione di protocollo tutti i documenti ricevuti e spediti dall'azienda compresi i documenti informatici dai quali possono nascere diritti, doveri e legittime aspettative di terzi.

Con la registrazione di protocollo si attribuisce al documento in arrivo o in partenza un valore giuridico probatorio

La registrazione di protocollo deve essere eseguita mediante la memorizzazione dei seguenti elementi:

1. numero di protocollo generato automaticamente e non modificabile dal sistema;
2. data della registrazione generata direttamente dal sistema e non modificabile;
3. mittente per il documento in arrivo e destinatario o destinatari per i documenti in partenza non modificabili dal sistema;
4. oggetto del documento registrato in modo non modificabile;
5. numero e descrizione degli allegati;
6. indicazione dei seguenti elementi del documento in arrivo: data e numero di protocollo;
7. impronta del documento informatico trasmesso via telematica. L'impronta è una sequenza di numeri binari che identifica in modo univoco il documento registrata in modo non modificabile.

CONTINUA.....

## DEFINIZIONI

**Area Organizzativa Omogenea (AOO):** è un insieme di uffici o unità organizzative o moduli o settori o servizi che usufruiscono, in modo omogeneo e ordinato degli stessi servizi per la gestione dei flussi documentali.

**Ufficio utente di una AOO:** ufficio dell'AOO che usufruisce del protocollo informatico messo a disposizione dalla stessa Area. I documenti protocollati sono sia quelli in entrata sia quelli in uscita, la successione numerica è unica ed è rinnovata ogni anno solare.

**Assegnazione di un documento:** è l'associazione del documento al responsabile del procedimento amministrativo (RPA).

**Aziende sanitarie e ospedaliere:** enti pubblici dotati di *personalità giuridica pubblica e autonomia imprenditoriale*. L'atto aziendale, di natura privatistica, ne disciplina l'organizzazione e la funzionalità.

Le AA. SS. e OO. sono gli strumenti di cui si serve lo Stato, per garantire al cittadino il suo diritto alla In tal senso lo Stato esercita la funzione pubblica in materia sanitaria.

**Casella istituzionale:** casella di posta elettronica dell'AOO abilitata a ricevere i messaggi da protocollare.

**Fascicolo:** insieme di documenti afferenti alla trattazione del medesimo affare o procedimento amministrativo.

**Fire wall** (muro di fuoco): sbarramenti software che proteggono il sistema (server, rete e terminali) da virus e da intrusioni illegali (hackers).

**Gestione dei documenti:** l'insieme delle attività effettuate mediante sistemi informativi automatizzati, che, nell'ambito del piano di classificazione, comprende la registrazione di protocollo, la classificazione, l'organizzazione, l'assegnazione e il reperimento dei documenti amministrativi-sanitari formati o acquisiti dall'Azienda.

**Registrazione di protocollo:** l'insieme di elementi (data di registrazione, numero di protocollo, mittente per il documento in arrivo e destinatario per il documento in partenza, oggetto, numero e descrizione degli allegati) che conferiscono al documento la rilevanza giuridico-probatoria. E' contestuale alla segnatura di protocollo ed è un atto pubblico.

**Responsabile del procedimento amministrativo:** la persona fisica responsabile degli adempimenti riguardanti, un affare o un procedimento amministrativo

**Scarto e selezione dei documenti:** l'operazione che consente l'eliminazione fisica dei documenti non più utili e l'individuazione di quelli soggetti a conservazione perenne.

**Segnatura di protocollo:** l'apposizione o l'associazione al documento originale, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

**Sistema di gestione informatica dei documenti:** l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche che consentono alle amministrazioni la gestione dei documenti.

**Titolario:** quadro alfanumerico che consente una sistemazione logica e gerarchica dei documenti in relazione alle funzioni aziendali

**Unità operativa responsabile (UOR):** l'ufficio, settore, unità operativa cui afferisce il responsabile del procedimento.

**Interoperabilità dei sistemi di protocollo informatico:** processo che consente l'interscambio di informazioni tra pubbliche amministrazioni, enti, cittadini, imprese (Massari)