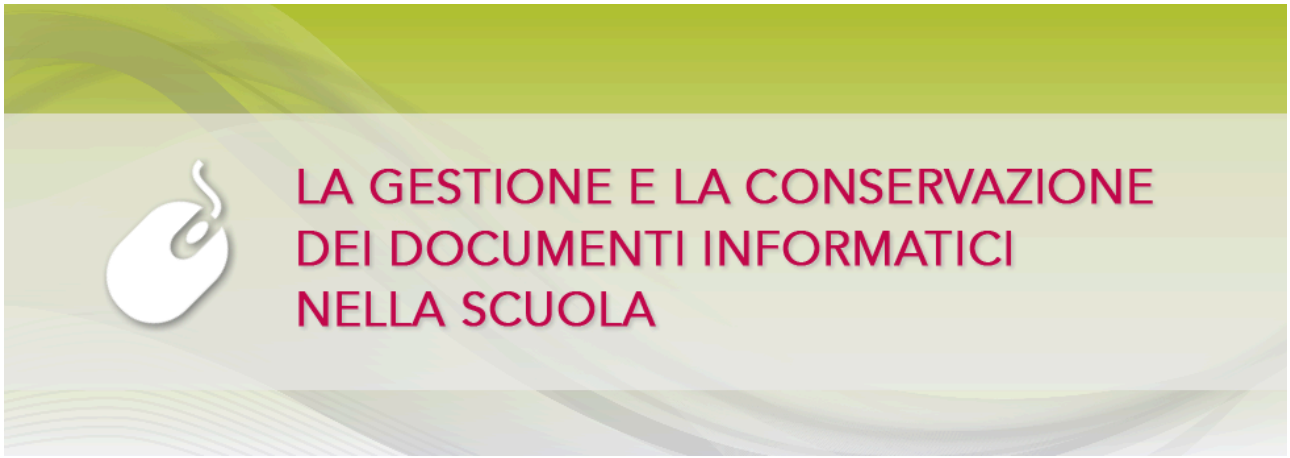
WBT DEL CORSO
“LA GESTIONE E LA CONSERVAZIONE DEI DOCUMENTI INFORMATICI NELLA SCUOLA”



Giugno 2016

Ed. 1 Rev.0/17-06-2016

Sommario

Introduzione al corso "La gestione e la conservazione dei documenti informatici nella Scuola"

Il percorso formativo sulla gestione documentale per le scuole rientra nell'ambito delle iniziative e degli interventi per la crescita delle competenze e della capacità tecnica dell'Amministrazione scolastica.

Le finalità di questo percorso, infatti, si pongono in linea di coerenza con i processi di modernizzazione e di rinnovamento della Pubblica Amministrazione in atto nell'ordinamento italiano ed europeo.

Come è noto, infatti, numerose azioni individuano il proprio obiettivo prioritario nel miglioramento della qualità del servizio scolastico attraverso interventi mirati su: qualità delle competenze professionali delle risorse umane che operano nel settore scolastico, qualità dell'offerta formativa, miglioramento di infrastrutture (come la connettività, le attrezzature didattiche e i laboratori).

Le tecnologie a scuola

Per le istituzioni scolastiche, l'informatica e la telematica non rappresentano soltanto una formidabile occasione per ripensare e rendere ancora più efficace l'attività didattica.

L'ingresso delle tecnologie dell'informazione e della comunicazione nei processi di lavoro ha permesso di ridefinire le modalità operative e la qualità dello scambio di informazioni tra amministrazioni, creando i presupposti logico-giuridici per il superamento di forme di "dialogo burocratizzato" tra cittadino e amministrazione, anche attraverso il completamento del sistema delle autocertificazioni.

La dematerializzazione dei documenti amministrativi, la gestione informatizzata delle informazioni in possesso dell'amministrazione, i sistemi di comunicazione sicura e certificata dei dati tra amministrazioni consentono, oltre ad una comunicazione più rapida ed efficiente, anche una verifica rapida, sicura e certificata delle dichiarazioni che il cittadino rilascia all'amministrazione pubblica.

Le norme della PA digitale

Le scuole possono cogliere i benefici derivanti dall'uso delle nuove tecnologie, solo rispettando le norme che da anni sono state dettate in materia di digitalizzazione dei procedimenti amministrativi e gestione documentale.

Infatti, in base all'art. 97, comma 1, della nostra Costituzione, le amministrazioni devono operare nel rigoroso rispetto delle disposizioni di legge, pena l'illegittimità della loro attività e dei loro atti.

Si tratta di norme, come il Codice dell'Amministrazione Digitale, che non possono essere ignorate, in quanto la loro violazione espone i dirigenti a sanzioni e responsabilità.

In questo scenario, il Codice dell'Amministrazione Digitale rappresenta il substrato su cui poggia l'intera architettura del modello disegnato dal legislatore, specificando gli aspetti tecnici e giuridici alla base dei nuovi strumenti di semplificazione. Il Codice, dunque, crea le condizioni giuridiche e organizzative per il percorso di innovazione intrapreso verso un'amministrazione digitale, efficiente e trasparente.

Da questa nuova organizzazione di strumenti e procedure, attraverso cui si esplica l'attività dell'amministrazione pubblica, discendono per i cittadini nuovi diritti (es. il diritto di autocertificare stati, qualità personali e fatti, il diritto di utilizzare le tecnologie informatiche nel dialogo con la PA, ecc.) rispetto ai quali la scuola è tenuta a fornire una risposta adeguata.

Perché usare le tecnologie a scuola

Questo processo di innovazione, che impatta su tutti i settori dell'Amministrazione Pubblica, investe sia l'organizzazione dei processi di lavoro sia le competenze in capo alle risorse umane sulle tematiche legate alla semplificazione e alla dematerializzazione di atti e procedure amministrative. Il rafforzamento di questo tipo di capacità incide sia sulla produttività del lavoro pubblico, sia sulle modalità di relazione con l'esterno (cittadini, imprese, altre PA), con incrementi sensibili in termini di efficienza e trasparenza dei servizi erogati.

I nodi da sciogliere verso una scuola digitale

L'amministrazione scolastica - così come l'intero universo delle PA - è chiamata a dare attuazione alle innovazioni introdotte dalla normativa e, pertanto, tenuta a dotarsi di una nuova architettura di Governance delle procedure interne e dei rapporti con l'utenza, non solo in funzione di un adeguamento formale al dettato normativo, quanto, piuttosto, per il raggiungimento degli obiettivi di semplificazione, efficienza, trasparenza, partecipazione e qualità del servizio, perseguiti dal legislatore.

Il punto di partenza di questa "rivoluzione copernicana digitale" è sicuramente rappresentato dalla dematerializzazione e rappresentato da una gestione completamente digitale di documenti, archivi e procedimenti.

Tale adeguamento non passa soltanto per l'acquisizione delle tecnologie necessarie, quanto-piuttosto – per l'acquisizione di una nuova cultura amministrativa e delle necessarie competenze digitali.

I contenuti del percorso formativo

Il Progetto si prefigge l'obiettivo di supportare la diffusione dell'innovazione delle prassi organizzative e gestionali degli istituti scolastici attraverso un percorso formativo sui nuovi principi dettati dalla normativa e sugli strumenti a supporto dei processi di digitalizzazione e dematerializzazione di procedure e di atti amministrativi.

Il progetto si propone di supportare l'avvio dei processi di digitalizzazione e semplificazione all'interno degli Istituti scolastici promuovendo, al contempo, la cultura dell'innovazione e la conoscenza degli strumenti giuridici e tecnici a supporto dei processi di dematerializzazione e de-certificazione di procedure e di atti amministrativi.

Il percorso formativo si prefigge di fornire ai destinatari una visione coordinata e d'insieme del disegno unitario di rinnovamento della PA, attuato attraverso le norme in tema di semplificazione e digitalizzazione e del relativo impatto in termini di efficienza, trasparenza e qualità del servizio reso a studenti e famiglie.

Premessa al Modulo 1. Dalla carta al bit: lo switch-off della PA digitale

La normativa inerente l'amministrazione digitale, ha segnato un netto cambiamento del modus operandi della Pubblica Amministrazione.

Il legislatore, ha inizialmente indicato alle Amministrazioni la possibilità di perseguire le proprie attività tradizionali, anche con gli strumenti dell'informatica:

- Firme elettroniche;
- Il documento informatico;
- La posta elettronica certificata;
- I siti web.

Successivamente tale bivalenza, è stata interrotta, imponendo un uso esclusivo degli strumenti informatici e digitali che hanno portato a un sostanziale cambiamento delle vecchie prassi amministrative.

Una volta che l'adeguamento al digitale sarà completo, perseguire nell'uso dei vecchi canali analogico/cartacei, denoterà automaticamente l'illegittimità dell'attività Amministrativa, ai sensi dell'articolo 97 comma1 della Costituzione secondo cui "*Le amministrazioni sono tenute a rispettare il principio di stretta legalità dell'azione amministrativa".* Per questo motivo tale attività, secondo quanto stabilito dal legislatore, è oggi informatica e digitale per definizione.

Nel corso di questo modulo si affronterà il tema dell'evoluzione normativa sull'informatica nella Pubblica Amministrazione, delineando il quadro di una riforma volta a semplificare le norme per gli uffici pubblici.

1 Introduzione alla normativa in materia di digitalizzazione della PA

1.1 Introduzione

L'e-Government non consiste nella mera automazione e meccanizzazione dell'attività dell'Amministrazione, ma nell'impiego "*delle ICT, ed in particolare di Internet, come strumenti per migliorarne l'efficienza e renderla maggiormente orientata alla soddisfazione degli utenti*".

Nel corso del presente modulo, sarà illustrato come le nuove tecnologie diventino il grimaldello per scardinare il vecchio ed inefficiente assetto burocratico e l'occasione per ripensare l'Amministrazione, innovandola sia sotto il profilo della razionalizzazione delle procedure interne (c.d. back office) sia sotto quello dei rapporti con l'utenza, mediante l'erogazione on line di vecchi e nuovi servizi (c.d. front office).

Si passerà poi ad esaminare l'evoluzione delle norme in materia di digitalizzazione dell'attività amministrativa, con l'elencazione dei principali atti normativi e delle disposizioni da essi introdotte.

Infine, si fornirà un quadro di sintesi delle novità che saranno introdotte in materia di dematerializzazione a seguito dell'attuazione delle disposizioni della recente Riforma della Pubblica Amministrazione sulla "Carta della Cittadinanza Digitale".

1.2 La Pubblica Amministrazione digitale

Costituisce principio ormai generalmente acquisito che l'uso dell'informatica e delle tecnologie dell'informazione e della comunicazione (ICT: Information&Communication Technologies) sia una delle principali soluzioni per uscire dalla grave crisi di risultati (e di credibilità) in cui versa l'Amministrazione.

Per questo, negli ultimi anni, si è assistito alla diffusione, sempre più capillare, delle tecnologie informatiche e telematiche negli uffici pubblici e nei processi di lavoro delle Amministrazioni.

Un'Amministrazione può dirsi realmente digitale solo quando i suoi processi prevedono l'impiego delle tecnologie dell'informazione e della comunicazione con i seguenti obiettivi:

- Accrescere l'efficienza;
- Ridurre i costi;
- Migliorare la qualità dei servizi resi all'utenza.

Tali obiettivi devono pertanto diventare i parametri alla luce dei quali misurare l'efficacia delle politiche pubbliche e delle azioni in concreto poste in essere dalle singole Pubbliche Amministrazioni.

Bisogna evitare che, nell'abbandono del cartaceo, si riproducano quei bizantinismi che l'introduzione delle nuove tecnologie ha lo scopo di evitare: ciò che nella modalità tradizionale è pratico e funzionale, in quella digitale potrebbe risultare farraginoso, se non addirittura irrazionale.

Si tratta di uno dei concetti cruciali che deve essere compreso dalle amministrazioni: l'informatizzazione tout court dei processi, senza una loro reingegnerizzazione, è destinata a non sortire alcun effetto positivo né in termini di efficienza, né in termini di trasparenza.

Il processo di digitalizzazione della PA presenta un triplice livello: tecnologico, organizzativo e normativo.

Da un lato, infatti, le amministrazioni devono inserire le tecnologie al posto dei tradizionali strumenti analogici utilizzati fin qui per la gestione dei procedimenti amministrativi di propria competenza.

L'uso degli strumenti tecnologici, però, deve essere rispettoso della normativa in materia dal momento che gli uffici pubblici sono tenuti al rispetto del principio di legalità dell'azione amministrativa sancito dall'art. 97 Cost.

Sono indubbie le implicazioni di carattere organizzativo di tale percorso: per cogliere appieno i vantaggi della digitalizzazione è infatti necessario che le amministrazioni pongano in essere una sostanziale revisione dei procedimenti amministrativi.

1.3 Il Codice dell'Amministrazione Digitale e le regole tecniche

In ambito pubblico, il processo di digitalizzazione deve necessariamente investire un triplice livello: tecnologico, organizzativo e giuridico-normativo, sempre con uno specifico riferimento sia ai principi sanciti a livello costituzionale dall'art. 97 in tema di imparzialità e buon andamento e sia con riferimento alle fonti normative che investono il processo di digitalizzazione della Pubblica Amministrazione.

In particolare, è sicuramente possibile affermare che – a seguito della rivoluzione tecnologica che ha riguardato tutti i settori della società – i canoni costituzionali di "imparzialità" e "buon andamento" possano essere assicurati solo attraverso l'uso delle nuove tecnologie per la gestione dei procedimenti amministrativi.

Dopo le riforme degli anni '90 si afferma la consapevolezza che le tecnologie ICT sono indispensabili alla Pubblica Amministrazione per rendersi cooperativa, federata a completo servizio dei cittadini; inizia ad affermarsi, anche a livello legislativo, il binomio tra P.A. e digitalizzazione, al punto da far affermare da più parti che la L.241/90 in tema di procedimento amministrativo, contenga modifiche all'assetto della P.A. conformi alle esigenze di informatizzazione.

Non è un caso che sia stata proprio la Legge n. 241/1990, all'art. 3-bis, a prevedere che, per conseguire maggiore efficienza nella loro attività, le Amministrazioni pubbliche dovessero incentivare l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati.

Non è un caso che le prime norme dell'Amministrazione digitale riguardino, appunto, l'introduzione e la disciplina del documento informatico e della firma digitale.

La disciplina del documento informatico e della sua validità giuridica hanno rappresentato il primo tassello per consentire l'applicazione analogica delle norme preesistenti alle nuove tecnologie. L'obiettivo del legislatore era consentire di conferire piena validità giuridica all'attività contrattuale e amministrativa svolta con l'ausilio degli strumenti informatici.

In base all'art. 50 D.P.R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), le Pubbliche Amministrazioni – e quindi anche le scuole - sono tenute a realizzare o revisionare i propri sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi fin dal 1° gennaio 2004.

Si tratta di uno dei primi obblighi a contenuto informatico per la PA: la piena operatività del protocollo informatico, infatti, può ben essere ritenuta la chiave di volta del sistema normativo in materia di digitalizzazione dei procedimenti amministrativi.

Non si tratta, infatti, di un intervento normativo dettato soltanto dai vantaggi, pure rilevanti, che possono derivare all'Amministrazione in termini economici e organizzativi, ma anche e soprattutto dalla presa d'atto che la strada verso il procedimento amministrativo elettronico e l'accesso telematico da parte dei cittadini passa necessariamente per la gestione informatizzata del registro di protocollo e degli archivi.

Con la legge n. 4/2004, il legislatore si è preoccupato di abbattere le barriere che limitano l'accesso dei soggetti diversamente abili alla società dell'informazione e che, conseguentemente, determinano perdita di opportunità e di partecipazione.

L'obbligo di garantire l'accessibilità degli strumenti informatici, e quindi dei siti Internet, non costituisce solo norma programmatica ma prescrizione dal chiaro nitore precettivo, dal momento che:

- sono nulli i contratti stipulati dalle Amministrazioni per "la realizzazione e la modifica di siti internet quando non è previsto che essi rispettino i requisiti di accessibilità stabiliti";
- la pubblicazione di documenti informatici non ha effetto se questi non sono conformi ai requisiti in materia di accessibilità.

Al fine di superare i limiti che la Posta Elettronica c.d. semplice ha nell'ambito dei rapporti giuridici (incertezza in merito ai momenti dell'invio e della ricezione e mancata verifica della provenienza) il legislatore italiano - con il DPR n. 68/2005 - ha introdotto nel nostro ordinamento l'istituto della

c.d. Posta Elettronica Certificata (PEC) quale strumento tecnico su cui costruire la trasmissione telematica dei documenti.

La PEC nasce con l'obiettivo di trasferire sul digitale il concetto di "Raccomandata con Ricevuta di ritorno" e superare, pertanto, le problematiche di certezza intrinseche della Posta Elettronica tradizionale. L'intenzione del legislatore è quella di fornire a privati e Pubblica Amministrazione uno strumento tecnologico in grado di conferire piena efficacia legale alla trasmissione dei documenti informatici.

Altro intervento normativo significativo è rappresentato dalla Legge n. 69/2009 in materia di pubblicazione degli atti delle amministrazioni.

In particolare, l'art. 32 riconosce l'effetto di pubblicità legale solamente agli atti e ai provvedimenti amministrativi pubblicati dalle amministrazioni sui propri siti istituzionali.

È espressamente sancito, infatti, che – a partire dal 1° gennaio 2011 - gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati.

A partire da tale data, le pubblicazioni effettuate in forma cartacea, invece, non hanno più effetto di pubblicità legale.

Il Codice dell'Amministrazione Digitale è stato emanato per conferire certezza e validità giuridica ai nuovi strumenti digitali e ampliare i nuovi diritti dei cittadini nell'uso delle tecnologie informatiche.

Le novità del Codice spaziavano dall'affermazione dei diritti dei cittadini di poter interloquire con le amministrazioni pubbliche attraverso l'uso della posta elettronica e di Internet, fino ad una radicale modifica delle modalità attraverso le quali gli enti devono provvedere alla gestione dei procedimenti amministrativi.

Il CAD:

- sancisce il diritto dei cittadini di interagire sempre, dovunque e verso qualsiasi Amministrazione attraverso Internet e posta elettronica;
- stabilisce che tutte le amministrazioni debbano organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale;
- ordina e riunisce norme già esistenti e ne introduce di nuove per nuovi servizi e nuove opportunità, ha creato insomma il quadro legislativo necessario per dare validità giuridica alle innovazioni;
- disegna una Pubblica Amministrazione che funzioni meglio e costi meno ai contribuenti;
- modifica radicalmente le modalità con cui gli enti devono provvedere alla gestione dei procedimenti amministrativi.

Il CAD non è stato compiutamente applicato dalle amministrazioni che, quindi, non hanno saputo cogliere le incredibili opportunità in termini di aumento di efficienza e migliore allocazione delle risorse; neanche i cittadini (probabilmente perché inconsapevoli) si sono attivati per far rispettare i nuovi diritti che, se effettivi, avrebbero potuto migliorare la loro qualità della vita.

Probabilmente anche a seguito di tali considerazioni, il CAD è stato oggetto di alcuni importanti interventi di modifica nei primi dieci anni di vita.

Le modifiche introdotte sono state molteplici ed hanno riguardato la necessità di un aggiornamento rispetto all'evoluzione tecnologica, un coordinamento con le ulteriori fonti del diritto riguardanti la Pubblica Amministrazione, nonché strumenti per fornire a cittadini ed imprese mezzi migliori per usufruire dei servizi on line.

Uno dei principali interventi normativi di modifica del Codice dell'Amministrazione Digitale è stato rappresentato dal Decreto Legge n. 179/2012 (c.d. "Decreto Crescita 2.0") in materia di Agenda Digitale Italiana.

L'Agenda Digitale Italiana rappresenta l'insieme di azioni e norme per lo sviluppo delle tecnologie, dell'innovazione e dell'economia digitale, in aderenza alla strategia Europa 2020, che fissa gli obiettivi per la crescita nell'Unione europea da raggiungere entro il 2020.

Il Decreto Crescita 2.0 contiene significative disposizioni in materia di:

- accessibilità dei documenti informatici delle pubbliche amministrazioni;
- obblighi di comunicazioni telematiche per le pubbliche amministrazioni;
- digitalizzazione dei contratti delle amministrazioni;
- valorizzazione del patrimonio informativo delle amministrazioni pubbliche.

Le disposizioni di principio contenute nel Codice dell'Amministrazione Digitale sono completate dalle regole tecniche e linee guida emanate sulla base di esso con distinti atti adottati dal Presidente del Consiglio (o dal Ministro delegato) e dall'Agenzia per l'Italia Digitale.

All'interno di questi atti sono contenute le specifiche modalità da rispettare per la digitalizzazione dei documenti e dei procedimenti amministrativi e l'indicazione della data entro cui tali modalità diventano cogenti.

Tra le diverse regole tecniche, le più significative in tema di dematerializzazione sono:

a) il DPCM 22 febbraio 2013 sulle firme elettroniche;

b) il DPCM 3 dicembre 2013 sul protocollo informatico e sulla gestione documentale;

c) il DPCM 3 dicembre 2013 sulla conservazione documentale;

d) il DPCM 13 novembre 2014 sul documento informatico.

1.4 La riforma della Pubblica Amministrazione e la carta della cittadinanza digitale

L'articolo 1 della Legge di Riforma della PA (Legge n. 124/2015, c.d. "Riforma Madia") contiene una delega al Governo in materia di erogazione di servizi da parte delle pubbliche amministrazioni ("uffici pubblici").

La delega dovrà contenere le modalità di erogazione dei servizi in via digitale ai cittadini, così da configurare una "cittadinanza digitale".

In particolare, la delega si pone due obiettivi:

- l'informatizzazione di documenti, pagamenti, servizi, nelle relazioni intrattenute dalle pubbliche amministrazioni con i cittadini, con l'obiettivo della totale accessibilità on line;
- la semplificazione organizzativa e decisionale delle pubbliche amministrazioni.

Sulla base dei principi forniti dal Parlamento art. 1 della Legge n. 124/2015, il Governo è chiamato ad adottare dei decreti di riforma del Codice dell'Amministrazione Digitale.

I principi e criteri direttivi da seguire nell'opera di modifica, integrazione, semplificazione del CAD sono destinati a portare cambiamenti significativi nel rapporto tra cittadini e Pubblica Amministrazione, nonché nella gestione ed organizzazione di quest'ultima (individuazione del livello minimo di sicurezza, qualità, fruibilità, accessibilità e tempestività dei servizi on line delle amministrazioni pubbliche; semplificazione e trasparenza dei procedimenti amministrativi mediante la digitalizzazione; definizione di criteri di digitalizzazione del processo di misurazione e valutazione della performance; adeguamento alle disposizioni adottate a livello europeo).

Premessa al Modulo 2. La centralità del CAD

La norma di riferimento per la Pubblica Amministrazione digitale, è il Codice dell'Amministrazione Digitale D.Lgl. 7 marzo 2005 n.82.

Esso è il punto di riferimento principale di tutte le pubbliche amministrazioni, per via delle regole tecniche che sono state approvate nel corso degli anni sulla base di quanto riportato in tale documento.

Il Codice dell'Amministrazione Digitale non è una norma sulla tecnologia; piuttosto è un documento che integra la Legge 241 del 1990, indicando le disposizioni sulla gestione dei procedimenti amministrativi di cui ciascun ufficio è competente.

Un procedimento amministrativo può considerarsi regolato prevalentemente da due entità normative:

- La Legge 241 che detta i principi generali del procedimento, gli istituti di partecipazione del privato e gli strumenti organizzativi;
- Il Codice dell'Amministrazione Digitale, che indica quali siano gli strumenti che le amministrazioni debbano tassativamente utilizzare per gestire i procedimenti amministrativi di cui sono competenti.

La conoscenza di un procedimento amministrativo presuppone dunque la conoscenza e, in gergo giuridico, il possesso dei concetti dell'Amministrazione digitale inseriti nel Codice e nelle regole tecniche.

2 Il Codice dell'Amministrazione Digitale

2.1 Introduzione

Nel corso del presente modulo sarà fornita un'introduzione al principale testo normativo sulla digitalizzazione del settore pubblico: il Codice dell'Amministrazione Digitale.

Il Codice e le sue regole tecniche rappresentano un corpo organico di disposizioni, che presiede all'uso dell'informatica come strumento privilegiato nei rapporti tra la Pubblica Amministrazione e i cittadini.

Dopo aver illustrato l'ambito di applicazione del CAD, saranno presentati i suoi principi e finalità, anche attraverso l'elencazione dei principali diritti digitali che il Codice conferisce a cittadini e imprese.
Si passerà poi ad esaminare più specificatamente le disposizioni che riguardano la dematerializzazione dell'attività amministrativa, con l'elencazione dei principali strumenti disciplinati dal legislatore (documento informatico, firme elettroniche, pec, protocollo informatico, ecc.).
Infine, si fornirà un quadro dei soggetti chiamati a rispondere dell'attuazione delle disposizioni del Codice dell'Amministrazione Digitale e dei diversi livelli sanzionatori che presidiano il corretto adempimento da parte delle pubbliche amministrazioni.

2.2 Principi e finalità

Con il Decreto Legislativo 7 marzo 2005 numero 82, è stato adottato il Codice dell'Amministrazione Digitale (CAD), ovvero un corpo organico di disposizioni relativo all'uso delle tecnologie info-telematiche nelle P.A.

Il CAD traccia il quadro normativo entro cui deve attuarsi la digitalizzazione dell'azione amministrativa e sancisce dei veri e propri diritti dei cittadini e delle imprese in materia di uso delle tecnologie nei rapporti con le amministrazioni; il CAD contiene anche l'obbligo per queste di snellire le procedure e di rendere tutti i servizi e le comunicazioni interne ed esterne per via telematica.

Il CAD è nato per conferire certezza e validità giuridica ai nuovi strumenti digitali e ampliare i nuovi diritti dei cittadini nell'uso delle tecnologie informatiche. Nella sua prima stesura prevedeva alcune importanti novità che spaziavano dall'affermazione dei diritti dei cittadini di poter interloquire con le amministrazioni pubbliche attraverso l'uso della posta elettronica e di Internet, fino ad una radicale modifica delle modalità attraverso le quali gli enti devono provvedere alla gestione dei procedimenti amministrativi.

Il Codice dell'Amministrazione Digitale:

- sancisce il diritto dei cittadini di interagire sempre, dovunque e verso qualsiasi Amministrazione attraverso Internet e posta elettronica;
- stabilisce che tutte le amministrazioni debbano organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale;
- ordina e riunisce norme già esistenti e ne introduce di nuove per nuovi servizi e nuove opportunità, ha creato insomma il quadro legislativo necessario per dare validità giuridica alle innovazioni;
- disegna una Pubblica Amministrazione che funzioni meglio e costi meno ai contribuenti;
- modifica radicalmente le modalità con cui gli enti devono provvedere alla gestione dei procedimenti amministrativi.

L'ambito di applicazione del Codice dell'Amministrazione Digitale è estremamente ampio e copre la totalità dei soggetti pubblici e privati che erogano servizi pubblici ed usano i soldi dei contribuenti.

In primo luogo, ai sensi dell'art. 2 CAD, le norme del Codice si applicano a tutte le Amministrazioni dello Stato, ivi comprese le Scuole di ogni ordine e grado, le Istituzioni educative, le Aziende e le Amministrazioni dello stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità Montane e loro consorzi e associazioni, le Istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio industria artigianato e agricoltura e loro associazioni; tutti gli Enti pubblici non economici nazionali, regionali e locali, le Amministrazioni, le Aziende e gli Enti del servizio sanitario nazionale.

Il CAD si applica anche alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della Pubblica Amministrazione.

L'entrata in vigore del Codice dell'Amministrazione Digitale, costituisce senza dubbio una delle più importanti innovazioni per la Pubblica Amministrazione, non solo perché vengono introdotti una serie di penetranti obblighi volti a reingegnerizzare le attività classicamente eseguite dalla P.A., ma anche perché, accanto a tali disposizioni, vengono previsti dei veri e propri diritti all'uso delle nuove tecnologie.

Le previsioni in tema di diritti digitali costituiscono un fondamentale traguardo per l'innovazione della Pubblica Amministrazione e possono rappresentare uno strumento di partecipazione molto forte per i cittadini, oltre che un istituto la cui applicazione potrebbe comportare un notevole incremento nella digitalizzazione dell'attività degli uffici pubblici.

Il Codice dell'Amministrazione Digitale enuncia nuovi diritti esigibili a vantaggio di cittadini e imprese nelle modalità di comunicazione con la PA. Si tratta dei c.d. *diritti digitali* che attengono a:

- **Diritto all'uso delle tecnologie:** cittadini e imprese possono richiedere ed ottenere che venga utilizzato il canale telematico nelle comunicazioni con le pubbliche amministrazioni e con gli altri soggetti individuati dalla legge (art. 3);

- **Partecipazione al procedimento amministrativo informatico:** le pubbliche amministrazioni devono garantire agli interessati l'esercizio in forma telematica dei diritti di partecipazione al procedimento amministrativo (art. 4);
- **Effettuazione dei pagamenti con modalità informatiche:** le pubbliche amministrazioni devono rendere possibile, sul territorio nazionale, l'effettuazione dei pagamenti in modalità elettronica (art. 5);
- **Comunicazioni tra imprese e amministrazioni pubbliche:** le comunicazioni tra le pubbliche amministrazioni centrali e le imprese devono avvenire esclusivamente in modalità telematica (art. 5-bis);
- **Utilizzo della posta elettronica certificata:** le Pubbliche Amministrazioni, per le comunicazioni telematiche che necessitano di una ricevuta di invio e di consegna, con i soggetti che hanno dichiarato preventivamente il proprio indirizzo, utilizzano la posta elettronica certificata (art. 6);
- **Qualità dei servizi resi e soddisfazione dell'utenza:** le amministrazioni pubbliche devono procedere alla riorganizzazione e all'aggiornamento dei servizi resi, sulla base delle reali esigenze e del grado di soddisfazione degli utenti (art. 7).

2.3 Obblighi in materia di dematerializzazione

L'intero concetto di Amministrazione Digitale ruota intorno a quella che viene chiamata "rappresentazione informatica" e che può essere definita come il risultato della trasformazione in bit di quegli atti, fatti o dati che possano avere rilevanza giuridica. La disciplina del documento informatico e della sua validità giuridica rappresenta il primo tassello per consentire l'applicazione delle norme preesistenti alle nuove tecnologie: l'obiettivo del legislatore è consentire di conferire piena validità giuridica all'attività contrattuale e amministrativa svolta con l'ausilio degli strumenti informatici.

Il Codice dell'Amministrazione Digitale fornisce poi gli strumenti per la gestione integralmente telematica dell'attività amministrativa e negoziale delle PPAA, in considerazione degli obblighi che impongono di abbandonare le tradizionali modalità analogiche, preoccupandosi di assicurare nel tempo l'affidabilità dei documenti e degli archivi.

L'introduzione delle tecnologie info-telematiche negli uffici pubblici deve essere necessariamente accompagnata dalla revisione delle strutture e dei modelli organizzativi esistenti, in quanto pensati per un'Amministrazione cartacea. Infatti, il mero utilizzo degli strumenti previsti dal CAD al posto di quelli tradizionali appare insufficiente a garantire il raggiungimento degli obiettivi perseguiti attraverso la digitalizzazione.
Nel modello individuato dal legislatore l'impiego delle tecnologie dell'informazione e della comunicazione costituisce uno dei momenti centrali del processo di riorganizzazione strutturale e gestionale delle pubbliche amministrazioni.

Si tratta di un processo piuttosto complesso, cogente per tutte le Amministrazioni pubbliche, teso a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la

modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese.

La Pubblica Amministrazione Digitale, nel rispetto delle norme dettate dal CAD, abbandona completamente le modalità tradizionali di formazione e gestione dei documenti e degli archivi.

Questo significa che tutti gli uffici devono dotarsi:

a) degli strumenti per la formazione dei documenti e la loro trasmissione (software per la redazione dei documenti, firme elettroniche per la sottoscrizione, recapiti di posta elettronica ordinaria e certificata per la trasmissione);

b) di sistemi informatici per la gestione dei documenti e dei fascicoli di procedimento (come il registro di protocollo informatico);

c) di sistemi di gestione e conservazione documentale che garantiscano di mantenere nel tempo la validità giuridica dei documenti e dei fascicoli.

L'attività della Pubblica Amministrazione si esplica tramite atti, categoria che abbraccia nel nostro ordinamento sia tutti gli atti posti in essere da una Pubblica Amministrazione nell'esercizio della propria potestà amministrativa sia tutti gli atti contrattuali.

Tradizionalmente, l'atto amministrativo assume una forma prestabilita che - nella maggior parte dei casi - è uno scritto autografo, in linguaggio naturale alfanumerico, formante un testo, riportato, di solito, su supporto cartaceo.

I nuovi strumenti informatici hanno smaterializzato il documento: il dato, l'informazione non sono più necessariamente legati ad un supporto, ma vivono, nascono, si trasmettono, si conservano indipendentemente da questo.

A seguito delle modifiche subite nel corso degli anni, il Codice dell'Amministrazione Digitale ha prescritto l'abbandono delle tradizionali modalità analogiche per la gestione delle attività delle pubbliche amministrazioni.

Sulla base di un vero e proprio meccanismo di switch-off, le disposizioni introdotte in tema di informatizzazione, non rivestono più il solo ruolo di dichiarazioni di intenti, ma devono essere attuate in tempi ben definiti, pena l'illegittimità dell'attività posta in essere dagli uffici.

A titolo esemplificativo, sulla base delle disposizioni già vigenti:

- gli accordi tra le pubbliche amministrazioni e i contratti per lavori, servizi e forniture possono essere stipulati solo in modalità digitale;
- le amministrazioni sono tenute ad inviare le proprie comunicazioni ad altre PA e imprese al loro recapito telematico;
- le amministrazioni sono tenute a trasmettere comunicazioni telematiche anche alle persone fisiche, nel caso in cui conoscano il loro recapito elettronico;

- le amministrazioni sono tenute a redigere i propri originali come documenti informatici e ad aprire un fascicolo informatico per ogni procedimento di propria competenza;
- le amministrazioni sono tenute ad avere un protocollo esclusivamente informatico e ad istituire un sistema di conservazione documentale per mantenere nel tempo la validità dei propri archivi informatici.

La dematerializzazione dell'attività amministrativa viene imposta dal legislatore per assicurare vantaggi sotto un triplice profilo:

a) organizzazione interna: la digitalizzazione è strumentale alla riorganizzazione dei processi e dei servizi;

b) rapporti con cittadini e imprese: la digitalizzazione è lo strumento per assicurare i diritti digitali degli utenti ai quali non può essere più richiesto di recarsi fisicamente presso gli uffici; a cittadini e imprese, infatti, andrà garantita la possibilità di effettuare la totalità delle operazioni attraverso l'uso di canali quali la Pec;

c) sicurezza: le modalità attraverso cui viene imposta la digitalizzazione hanno l'obiettivo di garantire la sicurezza di dati, documenti e sistemi, in considerazione della circostanza per cui atti ed archivi diventano solo informatici.

L'art. 41 del Codice dell'Amministrazione Digitale prevede che "le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente".

Questo significa che il procedimento amministrativo - inizialmente disciplinato con esclusivo riferimento alla carta dalla Legge n. 241/1990 - diviene integralmente informatico, in modo da rendere la Pubblica Amministrazione più efficiente, trasparente e capace di allocare in modo migliore le sempre minori risorse disponibili.

Tali obiettivi devono essere raggiunti con la sostituzione della carta e delle procedure analogiche con l'uso dell'informatica e della telematica e passano per un necessario adeguamento tecnologico ed organizzativo che presuppone la ridefinizione dei processi (c.d. reingegnerizzazione).

2.4 Sanzioni e responsabilità

Non risponde al vero la diffusa credenza per cui la violazione delle norme del Codice dell'Amministrazione Digitale, e in generale di tutte quelle in materia di informatizzazione del settore pubblico, non sia foriera di conseguenze per i singoli Enti (ed i loro dirigenti e funzionari).

Sotto questo profilo, è possibile individuare un duplice livello di responsabilità:

a) da un lato – in base all'art. 12, comma 1-ter CAD – tutti i dirigenti rispondono dell'adempimento delle disposizioni del Codice per quanto concerne le attività dei propri uffici;

b) dall'altro, esistono specifiche responsabilità che fanno capo a figure espressamente istituite per curare l'adempimento di specifiche disposizioni normative.

Le principali figure che vengono in rilievo sono:

- il responsabile della gestione documentale (DPCM 3 dicembre 2013)
- il responsabile della conservazione documentale (DPCM 3 dicembre 2013)
- il responsabile della sicurezza informatica (artt. 17 e 50-bis CAD)
- il responsabile della protezione dei dati personali (D. Lgs. n. 196/2003)

Tali figure possono essere ricoperte tutte dal Dirigente Scolastico che può delegare parte delle funzioni al Direttore dei Servizi Generali e Amministrativi - DSGA.

Fra le direttrici fondamentali su cui si muove la riforma del Codice dell'Amministrazione Digitale, una delle principali consiste nell'introduzione di previsioni dichiaratamente intese ad accrescere la tutela degli amministrati a fronte di ritardi e inefficienze dei soggetti pubblici nella digitalizzazione dei procedimenti amministrativi.

In tale prospettiva, accanto al riconoscimento esplicito di diritti a contenuto digitale degli utenti, si segnala l'espressa previsione secondo cui la mancata osservanza di tali norme può essere causa di responsabilità dei dirigenti amministrativi oltre alla circostanza per cui il livello di attuazione del CAD diventa elemento di valutazione della performance.

Inoltre, va osservato come l'impiegato pubblico è tenuto ad osservare il dovere di adempiere la prestazione con diligenza e quello di fedeltà all'Amministrazione datrice di lavoro: in particolare, l'inosservanza dei doveri inerenti all'ufficio da parte dell'impiegato pubblico determina la sua responsabilità disciplinare.

Questo significa che ogni pubblico dipendente deve contribuire, per la propria parte, all'attuazione del Codice dell'Amministrazione Digitale, al fine di evitare sanzioni e responsabilità.

Le norme del CAD attribuiscono al cittadino, alle imprese e ad ogni soggetto interessato, una posizione giuridica riconosciuta e tutelata nei confronti dell'Amministrazione.

La circostanza per cui la gran parte delle disposizioni del Codice non prevede specifiche sanzioni non deve trarre in inganno; infatti, a fronte di una posizione giuridica riconosciuta e tutelata del cittadino, non può non configurarsi una responsabilità della Pubblica Amministrazione nell'ipotesi in cui tale posizione venga lesa.

In particolare, la responsabilità può essere:

a) **civile:** l'ufficio può essere chiamato a rispondere dei danni patiti dall'utente che non è messo in condizione di utilizzare gli strumenti info-telematici previsti dal legislatore;

b) **penale:** il CAD impone l'uso delle nuove tecnologie per il compimento di una serie di atti (protocollo, formazione degli originali, albo, effettuazione delle comunicazioni) di conseguenza, continuare ad utilizzare gli strumenti analogico-cartacei, può comportare conseguenze penali;

c) **erariale:** l'intero processo di digitalizzazione dell'azione amministrativa risponde ad esigenze di riduzione dei costi legate al funzionamento degli uffici pubblici, le nuove tecnologie, infatti, consentono di effettuare le stesse attività, con un minor impiego di risorse (in termini economici e di personale).

Di conseguenza, la giurisprudenza contabile ha già sancito che sussiste la responsabilità per danno erariale a carico di quei soggetti che non abbiano proceduto alla digitalizzazione in modo corretto e conforme a quanto previsto dalle norme vigenti.

Premessa al Modulo 3. Il ciclo di vita del documento informatico

Uno dei concetti chiave della PA digitale, è la cosiddetta “dematerializzazione”, ovvero la sostituzione, e quindi la perdita di consistenza, di archivi e documenti cartacei in favore di quelli informatici.

Un documento informatico non va inteso diversamente solo per gli strumenti che ne permettono la creazione, ma anche per la gestione del suo ciclo di vita: formazione e/o acquisizione del documento, trasmissione, gestione e conservazione.

Tutti i documenti informatici della Pubblica Amministrazione devono essere in linea con la normativa sull’accessibilità, la Legge 4 del 2004 e i relativi provvedimenti di attuazione.

L’Amministrazione, solo a titolo di esempio, non può pubblicare sul proprio sito web scansioni di documenti cartacei, pertanto la generazione di originali informatici, rende l’Amministrazione non solo più efficiente a livello produttivo ed economico, ma anche più accessibile, in quanto consente che questi possano essere, da tutti, letti e compresi.

3 Il documento informatico

3.1 Introduzione

L'intero concetto di Amministrazione Digitale ruota, dunque, intorno al "documento informatico" che diviene lo strumento principale nella gestione dei procedimenti amministrativi.

L'attività amministrativa, ed in genere tutto il diritto amministrativo, è caratterizzata da un elevato livello di formalismo, per cui – nel corso del presente modulo - illustreremo come conferire legittimità ed efficacia probatoria ai documenti informatici formati dall'Amministrazione.

In particolare, dopo l'illustrazione delle tipologie di documento informatico e del loro valore giuridico, vengono passati in rassegna gli obblighi della Pubblica Amministrazione in materia di originali informatici.

Infine, viene affrontato il tema delle copie e duplicati di documenti informatici, analizzando la normativa contenuta nelle regole tecniche adottate con DPCM 13 novembre 2014.

3.2 La nozione di documento informatico

L'attività della Pubblica Amministrazione si esplica tramite atti, categoria che abbraccia nel nostro ordinamento, sia tutti gli atti posti in essere da una Pubblica Amministrazione nell'esercizio della propria potestà amministrativa, sia tutti gli atti contrattuali.

Tradizionalmente, l'atto amministrativo assume una forma prestabilita che - nella maggior parte dei casi - è uno scritto autografo, in linguaggio naturale alfanumerico, formante un testo, riportato, di solito, su supporto cartaceo.

Le nuove tecnologie, e soprattutto l'informatica, hanno dematerializzato il documento: il dato, l'informazione non sono più necessariamente legati ad un supporto, ma vivono, nascono, si trasmettono, si conservano indipendentemente da questo; insomma, non hanno più bisogno di essere abbinati a una cosa materiale (la carta) determinata e definita.

La dematerializzazione del documento rende inservibili tutte quelle regole atte a dare certezza della provenienza e dell'autenticità dei contenuti dell'atto amministrativo che si erano costruite attorno all'elemento materiale del documento.

Il legislatore ha dovuto dettare nuove regole per ridefinire il concetto stesso di documento e, per quel che più interessa, di documento amministrativo, e riprodurre tali garanzie; in altre parole ha dovuto elaborare un concetto di documento informatico che offrisse le stesse garanzie del documento cartaceo.

L'attribuzione di rilevanza giuridica ai documenti informatici attraverso un'apposita normativa, ha costituito il primo tassello per la costruzione di un'era tecnologica, non solo nell'ambito della Pubblica Amministrazione, ma in ogni settore della vita sociale.

Tale disciplina è stata inizialmente introdotta a partire dal 1997, mentre prima di allora, di fronte agli esempi concreti della tecnologia informatica o telematica, non vi erano certezze dal punto di vista giuridico.

La prima norma in materia è stato l'art. 15, comma 2, Legge n. 59/1997 che ha introdotto l'innovativo principio per cui: "Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge".

Attualmente, la normativa in materia di documento informatico è contenuta nel Codice dell'Amministrazione Digitale e nelle Regole tecniche emanate con DPCM 13 novembre 2014.

Nel nostro ordinamento, la nozione "tradizionale" di documento amministrativo è contenuta all'art. 1 del DPR n. 445/2000 (Testo Unico sulla Documentazione Amministrativa).

Esso è definito come "ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa".

La nozione di documento è la più ampia possibile, così come dimostrato anche dall'art. 22 Legge n. 241/1990 in base al quale "è considerato documento amministrativo ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie*".*

L'introduzione delle tecnologie info-telematiche negli uffici pubblici deve essere necessariamente accompagnata dalla revisione delle strutture e dei modelli organizzativi esistenti, in quanto pensati per la nozione di documento informatico, ricalcata su quella del documento analogico, come la più ampia possibile; pertanto, in base a quanto previsto dall'art. 1 CAD, possiamo definire il documento informatico come la "rappresentazione informatica" del contenuto di atti, fatti o dati giuridicamente rilevanti.

L'intero concetto di documento informatico ruota, dunque, intorno a quella che viene chiamata "rappresentazione informatica" e che può essere definita come il risultato della trasformazione in bit, e successiva memorizzazione (ad esempio su un server o un DVD), di quegli atti, fatti o dati che possano avere rilevanza giuridica.

Uno degli aspetti maggiormente rilevanti legati alla dematerializzazione dell'attività amministrativa è quello relativo all'efficacia giuridica dei documenti informatici.

Sotto questo profilo, il Codice dell'Amministrazione Digitale differenzia il valore dei documenti informatici in base al tipo di sottoscrizione:

a) **Documento informatico non sottoscritto:** il documento informatico semplice, non sottoscritto - cioè - con firme elettroniche, ha una scarsa efficacia probatoria e può ritenersi che faccia piena prova dei fatti e delle cose rappresentate, solo se colui contro il quale è prodotto non ne disconosce la conformità ai fatti o alle cose medesime;

b) **Documento informatico sottoscritto con firma debole:** il documento informatico cui è apposta una firma debole, sul piano probatorio, è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Spetterà al soggetto che lo ha prodotto dimostrare, di volta in volta, l'affidabilità del documento;

c) **Documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale:** il Codice dell'Amministrazione Digitale prevede che il documento sottoscritto con firma elettronica avanzata, qualificata o digitale abbia - sul piano probatorio - l'efficacia prevista dall'art. 2702 del Codice Civile in base al quale "la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta".

3.3 La formazione del documento informatico

Il CAD contiene la disciplina dell'intero ciclo di vita del documento informatico e sancisce la sua validità e rilevanza con riferimento alla sua formazione, trasmissione, gestione e conservazione nel tempo.

Una volta rispettate le regole tecniche dettate dal DPCM 13 novembre 2014, il documento informatico, formato, trasmesso e conservato con strumenti telematici ha identica validità, ad ogni effetto di legge, del documento cartaceo e deve essere accettato da qualsiasi soggetto pubblico o privato.

Dopo aver assicurato al documento informatico gli stessi requisiti di affidabilità, il legislatore ha dedicato una disposizione molto importante agli originali dei documenti delle Pubbliche Amministrazioni.

Infatti, l'art. 40, comma 1, CAD prevede che "le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici" nel rispetto delle regole tecniche definite con DPCM 13 novembre 2014.

Dal momento che le regole tecniche dovranno necessariamente essere recepite entro 18 mesi dalla loro entrata in vigore, questo significa che le Pubbliche Amministrazioni potranno – a far data dall'11 agosto 2016 – formare legittimamente solo originali informatici (a pena di illegittimità dell'atto amministrativo).

Si tratta di una norma generale che si applica a tutti gli atti delle PA, fatta eccezione dove il legislatore abbia previsto un regime diverso.

Due esempi particolarmente rilevanti sono i contratti tra pubbliche amministrazioni (art. 15 Legge n. 241/1990) e i contratti per lavori, servizi e forniture (art. 44 D. Lgs. n. 50/2016) che devono essere sottoscritti necessariamente in digitale.

Le quattro modalità di formazione cui le Pubbliche Amministrazioni sono tenute a conformarsi nella redazione dei documenti informatici sono contenuti all'art. 3 DPCM 13 novembre 2014.

La prima, e una delle più frequenti, è rappresentata dalla redazione tramite appositi strumenti software (ad esempio, documenti di testo, fogli di calcolo, schemi XML).

Le Regole Tecniche prevedono che siano equiparate alla redazione tramite apposito software anche:

- l'acquisizione di un documento informatico per via telematica (ad esempio attraverso posta elettronica ordinaria o certificata) o su supporto informatico (es. consegnato su supporto magnetico);
- l'acquisizione della copia per immagine su supporto informatico di un documento analogico (ad esempio tramite scansione) e l'acquisizione della copia informatica di un documento analogico.

L'introduzione delle tecnologie info-telematiche negli uffici pubblici deve essere necessariamente accompagnata dalla revisione delle strutture e dei modelli organizzativi esistenti in quanto pensati per un documento analogico. Altra tipologia rilevante di documento informatico, specialmente per i servizi in rete, è rappresentata dalla registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente.

Attraverso tale modalità, l'invio di dati attraverso la compilazione di un *form* è considerata equivalente all'invio via PEC di un documento (naturalmente, a parità di certezza in ordine all'identità dell'utente).

Altra tipologia di documento informatico è quella ottenuta attraverso la generazione o il raggruppamento – anche in via automatica – di un insieme di dati o registrazioni provenienti da una o più banche dati raggruppati secondo una struttura logica determinata.

Questo tipologia è molto importante in quanto consente di conferire validità giuridica a tutti gli scambi di documenti e di informazioni in regime di cooperazione applicativa.

Le norme, ai fini dell'efficacia giuridica del documento informatico, attribuiscono centralità alle sue caratteristiche di immodificabilità e integrità.

Le Regole tecniche chiariscono che tali requisiti sono assicurati da una o più delle seguenti operazioni:

a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata

b) l'apposizione di una validazione temporale

c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa

d) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza

e) il versamento ad un sistema di conservazione.

Al momento della formazione del documento informatico, è necessario fare attenzione ai metadati dello stesso.

Per metadati si intende un insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

Le Regole tecniche contengono l'indicazione dei metadati minimi che devono essere associati a ogni documento formato dall'Amministrazione.

3.4 Copie e duplicati

Una volta definite le regole per la formazione dei documenti informatici, il legislatore ha disciplinato la transizione dalla carta al bit (e viceversa) fin tanto che tutti gli utenti dell'Amministrazione saranno obbligati a dotarsi di strumenti informatici per la redazione e trasmissione dei documenti.

La definitiva sistematizzazione della normativa sul ciclo di vita del documento informatico consente di sostituire con copie digitali i documenti amministrativi cartacei.

A tal fine, il Codice dell'Amministrazione Digitale distingue tra due tipi di copie:

a) la copia informatica di documento analogico: definita come "il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto" (art. 1, comma 1, lett. i-bis);

b) la copia per immagine su supporto informatico di documento analogico: definito come "il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto" (art. 1, comma 1, lett. i-ter).

Il legislatore conferisce a queste copie la stessa efficacia probatoria degli originali che sostituiscono se sono accompagnate dall'attestazione di conformità all'originale cartaceo da cui sono estratte.

Con il Codice dell'Amministrazione Digitale, nella gestione dei procedimenti amministrativi, il documento informatico diventa la regola e il cartaceo l'eccezione.

Questo significa che l'Amministrazione dovrà utilizzare sempre il digitale, formando con i nuovi strumenti gli originali dei propri atti e documenti; tali atti dovranno essere comunicati e notificati sempre in modalità telematica.

Nei casi in cui questo non sia possibile, il legislatore ha previsto la possibilità per l'ente di utilizzare la carta, in modo residuale. Risponde a questa finalità la disciplina della "copia analogica di originale informatico" che viene definita come "il documento su carta avente contenuto identico a quello del documento informatico da cui è tratto". Per garantire piena efficacia giuridica, è previsto che un pubblico ufficiale debba attestare la conformità all'originale informatico da cui è tratto.

La certificazione di conformità non è necessaria solo nel caso in cui la copia a stampa dell'originale informatico debba essere trasmessa ad un cittadino sprovvisto di domicilio digitale; in questo caso, ai sensi dell'art. 3-bis, comma 4-bis del CAD, sarà sufficiente l'indicazione a mezzo stampa del firmatario.

Il legislatore si preoccupa anche di dettare disposizioni in materia di duplicati e copie digitali di documenti informatici e, in particolare, definisce:

a) la "copia informatica di documento informatico" come il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (art. 1, comma 1, lett- i-quater);

b) il "duplicato informatico" come il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (art. 1, comma 1, lett. i-quinquies).

Il duplicato consiste, quindi, nella produzione di un documento informatico del tutto identico a quello, sempre informatico, da cui è tratto e dal quale, in concreto, non è distinguibile; al contrario, la copia informatica di un documento informatico consiste in un documento informatico che viene tratto da un originale (ovviamente informatico) da cui resta, però, distinguibile (perché, per esempio, si utilizza un diverso formato, come nel caso di una copia in formato .pdf di un originale in .doc). Dal punto di vista pratico, i duplicati, per la loro indistinguibilità dall'originale, li sostituiscono a ogni effetto, mentre le copie non fanno venir meno l'obbligo di conservazione dell'originale.

Premessa al Modulo 4. Ad ogni atto la sua firma

L'efficacia giuridica di un documento è strettamente correlata al tipo di sottoscrizione che gli è abbinata.

Il legislatore, infatti, ricollega l'efficacia giuridica del documento informatico, al tipo di sottoscrizione elettronica che gli è abbinata prevedendo, quindi, quattro differenti tipologie di firma elettronica:

La firma elettronica debole;

La firma elettronica avanzata;

La firma elettronica qualificata;

La firma elettronica digitale, che rappresenta lo strumento più affidabile di firma digitale, sia dal punto di vista tecnico che normativo.

Esistono infatti molti precedenti giurisprudenziali che permettono di inserire questa tipologia di sottoscrizione elettronica nell'attività amministrativa. La firma digitale dovrà essere la scelta preferita, laddove l'amministrazione debba adottare degli atti che la impegnino all'esterno, come ad esempio nei contratti o comunque quando l'amministrazione debba esprimere manifestazioni di volontà.

La normativa sulle firme elettroniche, il Codice dell'Amministrazione Digitale e le regole di esecuzione, non illustrano soltanto la tecnologia ma anche il modo di adoperarla, ad esempio suggerendo di non far utilizzare ad altri il nostro dispositivo di firma digitale. È importante comprendere che l'utilizzo di quel dispositivo sia riservato al suo possessore.

4 Le firme elettroniche

4.1 Introduzione

Il valore giuridico dei documenti informatici è diretta conseguenza della tipologia di firma elettronica con la quale il documento è stato sottoscritto dal firmatario.

Per questo motivo, nel presente modulo didattico, dopo aver passato in rassegna l'evoluzione normativa in materia, saranno presentate le diverse tipologie elettroniche, cercando di delineare le differenze tra le varie categorie.

Inoltre, dopo aver illustrato le regole in materia di firma, rilevanti per gli istituti scolastici, sarà presentato il recente Regolamento dell'Unione Europea n. 910/20 (c.d. EIDAS) che – dettando un'unica disciplina per tutti i Paesi dell'Unione – introduce anche alcune significative novità.

4.2 Introduzione alle firme elettroniche

Nel mondo analogico, si era abituati a conoscere ed usare un unico tipo di firma, ossia quella autografa apposta sulla carta, e si è abituati a riconoscerle il significato giuridico per il quale l'apposizione di essa in calce ad una dichiarazione ha lo scopo di attestare - fino a prova contraria - la provenienza delle dichiarazioni in essa contenute.

Nel mondo della carta, la sottoscrizione autografa (cioè la firma) apposta dal privato in calce al documento esprime sino a prova contraria il consenso del firmatario sul contenuto dell'atto sottoscritto.

Nel mondo informatico, invece, il problema della sottoscrizione elettronica viene affrontato e risolto in modo sostanzialmente differente con le firme elettroniche.

Con l'avvento delle firme elettroniche si deve modificare il modo di intendere il concetto di sottoscrizione.

Le firme elettroniche non riproducono il nome e il cognome del firmatario, non sono costituite da parole, né da disegni, non sono apposte manualmente; si tratta piuttosto di sottoscrizioni che, in forma di bit, conferiscono determinati effetti ad un dato documento informatico.

Il sistema delle firme elettroniche trova oggi nel CAD un nuovo assetto. Si parla di "firme elettroniche" in quanto il legislatore prevede quattro tipologie di sottoscrizione informatica (firma elettronica, firma elettronica avanzata, firma elettronica qualificata e firma digitale) che si differenziano sia dal punto di vista tecnico sia da quello dell'efficacia giuridica.

La disciplina giuridica delle firme elettroniche viene posta attraverso due interventi:

- l'individuazione e definizione della procedura tecnica, tra le diverse disponibili, per garantire provenienza e autenticità del documento informatico;
- il trasferimento delle tutele giuridiche proprie della sottoscrizione autografa a tale procedura.

In relazione a tale normativa, le amministrazioni sono chiamate ad un doveroso duplice adeguamento:

- tecnologico: gli enti devono acquisire gli strumenti informatici necessari (supporti, software, dispositivi di firma);
- organizzativo: per ciascun procedimento, si rende necessario capire quale tipo di sottoscrizione elettronica deve essere utilizzata per conferire all'attività digitale gli stessi requisiti dell'attività tradizionale.

In particolare è possibile distinguere tra due macro-tipologie di firme elettroniche:

a) **le " firme deboli" (firma elettronica):** consentono di ricondurre in qualsiasi forma dei dati elettronici, ad esempio una firma a stampa, ad un soggetto, ma non assicurano l'integrità del documento stesso. Il documento è liberamente valutabile in giudizio, tenendo conto delle sue caratteristiche oggettive di qualità e sicurezza;

b) **le "firme forti" (firma elettronica avanzata, firma elettronica qualificata e firma digitale):** sono quelle per cui il firmatario non può disconoscere semplicemente la sottoscrizione se non a querela di falso. Garantiscono l'identità dell'autore e l'integrità del documento firmato.

4.3 Le firme elettroniche nella legislazione italiana

La firma elettronica semplice è data dall'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica. Tale tipo di sottoscrizione, ad esempio, può consistere anche in una semplice password o pin che siano idonei all'identificazione informatica del firmatario di un documento oppure nella scansione della firma autografa apposta su carta.

Si tratta di una tipologia di sottoscrizione particolarmente eterogenea, in cui sono ricompresi sia meccanismi che utilizzino accorgimenti in grado di dare solo minime certezze sulla identità del sottoscrittore e/o integrità del documento, sia tecnologie che garantiscono un alto grado di sicurezza informatica.

La firma elettronica avanzata può essere realizzata con tecnologie differenti ma deve sempre garantire:

a) l'identificazione del firmatario del documento;

b) la connessione univoca della firma al firmatario;

c) il controllo esclusivo del firmatario del sistema di generazione della firma;

d) la possibilità di verificare che il documento non abbia subito modifiche dopo l'apposizione della firma;

e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

f) l'individuazione del soggetto che eroga le soluzioni di firma elettronica avanzata.

La firma grafometrica è una definizione comunemente usata per indicare una modalità di firma elettronica realizzata con un gesto manuale del tutto analogo alla firma autografa su carta. I dati di una firma si acquisiscono mediante un dispositivo in grado di acquisire dinamicamente il movimento di uno stilo - azionato direttamente dalla mano di una persona - su una superficie sensibile (emulando una penna sulla carta).

Se rispetta i requisiti previsti dalle Regole Tecniche, la firma grafometrica può avere l'efficacia di firma elettronica avanzata.

Il Codice dell'Amministrazione Digitale definisce la "firma elettronica qualificata" come un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma. Tale tipologia di firma consente, rispettivamente, di avere certezza non solo in relazione all'imputabilità di un determinato documento ma anche in relazione alla sua integrità.

La firma qualificata si differenzia dalla firma elettronica avanzata per la presenza di un certificato, e dalla firma digitale in quanto tale certificato, cosiddetto qualificato, è diverso da quello che la norma associa alle firme digitali.

La firma digitale costituisce il metodo di sottoscrizione più sicuro e consolidato rispetto a quelli precedentemente descritti. In base al CAD, essa costituisce, infatti, un tipo particolare di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Il legislatore italiano ha disciplinato la firma digitale come principale strumento in grado, allo stato attuale della tecnologia, di assicurare l'integrità e la provenienza dei documenti informatici, e – conseguentemente – ad attribuire particolare valenza giuridica a questa modalità di sottoscrizione.

La firma digitale (secondo la definizione data all'art. 1, comma 1, lett. s, CAD) è il risultato di una complessa procedura informatica di validazione di un documento informatico per mezzo della quale - attraverso l'utilizzo di una doppia chiave di cifratura (una pubblica ed accessibile, l'altra rigorosamente privata e segreta) -, è possibile attribuire paternità e immodificabilità al documento stesso.

È opportuno chiarire, per evitare equivoci e fraintendimenti che la firma autografa e la firma digitale sono due cose sostanzialmente diverse:

a) la firma autografa è un "segno" che una persona appone in calce alle proprie dichiarazioni con lo scopo di attestare, attraverso la riconoscibilità della grafia, la personale provenienza della dichiarazione stessa;

b) la firma digitale, invece, è un metodo informatico di attribuzione della paternità e di garanzia della riservatezza di un documento informatico che si basa su un procedimento tecnico fondato sui principi individuati dalla crittografia moderna e regolamentati dal CAD e dalle sue regole tecniche.

L'appartenenza di una coppia di chiavi ad un determinato soggetto è assicurata da un apposito Certificatore iscritto in un apposito elenco tenuto dall'Agenzia per l'Italia Digitale.

Il Certificatore è una "terza parte fidata" la quale è incaricata di garantire, sia nella fase della generazione della coppia di chiavi e dell'attribuzione delle stesse ad un soggetto, sia nella successiva fase di verifica della titolarità della firma digitale apposta, l'identità del sottoscrittore.

Il CAD stabilisce precisi requisiti (giuridici, di onorabilità, di competenza ed esperienza dei responsabili tecnici, nonché di conformità di processi e prodotti informatici a standard riconosciuti di qualità) per l'esercizio dell'attività di certificazione, ai fini della validità legale della firma digitale. E' richiesto inoltre che il soggetto certificatore sia incluso in un elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura dell'Agenzia per l'Italia Digitale.

I documenti informatici possono essere sottoscritti con diverse modalità previste dal Manuale per la gestione dei flussi documentali delle scuole e in particolare:

a) firma a mezzo stampa (ai sensi dell'art. 3 del decreto legislativo 29 del 1993);

b) firma elettronica semplice;

c) firma elettronica avanzata;

d) firma elettronica qualificata;

e) firma digitale conforme alla normativa vigente rilasciata da una *Certification Authority* accreditata dall'Agenzia per l'Italia Digitale.

La sottoscrizione elettronica è elemento che condiziona il valore legale di un documento informatico.

Per questo motivo, all'interno del Manuale di gestione documentale dell'Istituto Scolastico (da adottarsi ai sensi dell'articolo 5 del DPCM 3 dicembre 2013) dovrà prevedersi che - in caso di documenti ricevuti - prima di procedere alla registrazione di protocollo si debba verificare la validità della sottoscrizione.

Per la verifica della firma digitale possono essere utilizzati i software e gli strumenti on line gratuitamente resi disponibili sul sito dell'Agenzia per l'Italia Digitale.

4.4 Il regolamento EIDAS

Il 28 agosto 2014 è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il Regolamento numero 190 del 2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Il Regolamento noto con l'acronimo EIDAS (*Electronic Identification Authentication and Signature*), stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e sancisce le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche.

Il provvedimento permetterà, in modo progressivo, di adottare a livello europeo un quadro tecnico-giuridico unico, omogeneo e interoperabile in ambito di firme elettroniche e autenticazioni elettroniche.

Sicurezza, certezza giuridica, affidabilità, facile impiego, riservatezza e regole comuni adottate in un mercato unico, come quello europeo, sono divenuti, infatti, requisiti fondamentali e necessari nelle transazioni elettroniche tra imprese, Pubbliche Amministrazioni, professionisti e cittadini.

Numerose sono le novità introdotte dal Regolamento EIDAS.

Una delle più significative è rappresentata dall'introduzione del sigillo elettronico (anche qualificato) della persona giuridica, inteso come prova dell'emissione di un documento da parte di una persona giuridica (garantendo certezza dell'origine e integrità del contenuto).

Inoltre, il Regolamento prevede che un documento su cui sono apposti una firma elettronica qualificata o un sigillo elettronico qualificato della persona competente per rilasciarlo gode della presunzione legale di integrità dei dati e di correttezza dell'origine di quei dati a cui la firma o il sigillo elettronico qualificato sono associati.

Molto significativa anche l'affermazione del principio per cui ad un documento elettronico non possono essere negati gli effetti giuridici e l'ammissibilità, come prova in procedimenti giudiziali, per il solo motivo della sua forma elettronica.

Premessa al Modulo 5. La gestione dei documenti e il procedimento amministrativo informatico

Documento informatico e firme elettroniche non sono sufficienti per individuare un'amministrazione digitale. Una volta ricevuto un documento o atto esterno sottoscritto, infatti, è necessario un archivio digitale in cui inserirlo, in modo che sia coerentemente incluso e collegato con tutte le altre pratiche relative a quel procedimento amministrativo.

Tale archivio è definito "Sistema di Gestione Documentale", normato a partire dal Testo Unico sulla documentazione amministrativa, dal codice dell'Amministrazione Digitale e dalle sue Regole Tecniche. L'Archivio è lo strumento indispensabile per la gestione dei documenti informatici in tutto il ciclo del procedimento amministrativo.

Il Sistema deve essere dunque collegato a profili di ordine tecnologico e organizzativo, per questo è prevista una rete di personalità responsabili coordinate da un unico soggetto. A tal fine, sono contemplati anche dei manuali di procedura, che devono essere continuamente aggiornati e doverosamente rispettati da chi lavora all'interno dell'Amministrazione.

5 Il sistema di gestione documentale

5.1 Introduzione

La digitalizzazione dell'attività amministrativa è resa possibile solo dalla dematerializzazione dei documenti e degli archivi e, quindi, dall'implementazione di un sistema di gestione dei documenti che consenta di perseguire obiettivi di risparmi, efficienza e trasparenza.

L'erogazione dei servizi in rete e la riorganizzazione degli uffici presuppone infatti nuove modalità di formazione, smistamento e archiviazione dei documenti.

Nel presente modulo, dopo la definizione delle attività demandate al sistema di gestione documentale, verrà illustrata la normativa vigente che pone precisi adempimenti tecnologici ed organizzativi in capo alle Pubbliche Amministrazioni.

Ci si soffermerà particolarmente sulla descrizione delle figure coinvolte nelle attività di gestione documentale e sulle rispettive responsabilità. Saranno poi menzionati i principali contenuti dei Manuali di gestione dei flussi documentali e degli archivi.

5.2 Gli obblighi normativi in materia di gestione documentale

Contrariamente a quanto possa pensarsi, le maggiori criticità legate alla dematerializzazione dei documenti e degli archivi non sono soltanto di tipo tecnologico, ma anche – e forse soprattutto di tipo organizzativo.

Non solo, nel passaggio al documento informatico, si è riscontrata una scarsa sensibilità degli utenti per i principi della gestione archivistica dei documenti, ma – molto spesso – si è assistito all'adozione di scelte organizzative assai eterogenee.

Per questo motivo il legislatore ha deciso di istituire in ogni Amministrazione un sistema informatizzato per la gestione dei flussi documentali, come insieme delle tecnologie e delle procedure utilizzate dagli uffici per la gestione dei propri documenti.

Il sistema di gestione documentale è l'insieme dei documenti e della logica archivistica (infrastrutture, organizzazione e classificazione) che caratterizzano la gestione documentale derivante dall'attività di un singolo o un'organizzazione.

Da questa definizione possiamo dedurre che il sistema documentale può essere scomposto in tre elementi fondamentali: i documenti prodotti e acquisiti dall'Amministrazione nell'ambito dello svolgimento delle proprie funzioni; l'infrastruttura di gestione in termini di tecnologie, regole e protocolli.

Il fine ultimo di un sistema documentale è quella di fornire un supporto documentale che sia efficace, trasparente e che garantisca una corretta conservazione e una rapida e sicura fruizione dei documenti prodotti e ricevuti.

La scienza archivistica definisce come archivio il "complesso organico di documenti prodotti da un determinato ente nell'esercizio delle sue funzioni istituzionali".

Il Testo Unico sulla documentazione amministrativa distingue l'archivio corrente dall'archivio di deposito, e questi dall'archivio storico. Ciascun archivio corrisponde ad una fase della vita del documento.

L'archivio corrente contiene i fascicoli ancora aperti, ossia quelli relativi a procedimenti non ancora conclusi.

La funzione prevalente dell'archivio corrente è duplice: da un punto di vista amministrativo-gestionale, l'archivio corrente svolge la finalità di offrire all'Ente il necessario supporto informativo per la regolare azione amministrativa; dal punto di vista archivistico serve per "regolare il processo di sedimentazione delle carte in modo da ritrovare rapidamente e con certezza i documenti quando servono".

L'archivio di deposito raccoglie la documentazione relativa ad affari chiusi e la cui integrale tenuta sia ancora utile ai fini giuridici ed amministrativi da parte del soggetto produttore. Tale documentazione viene di regola conservata nell'archivio di deposito per un tempo definito dalla chiusura dell'affare. Entro il predetto termine, la documentazione viene sottoposta a procedimento di scarto, previa autorizzazione della Soprintendenza, ovvero al versamento presso l'Archivio Storico competente.

Il Testo unico sulla documentazione amministrativa prevede che ciascuna Amministrazione debba istituire un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi per ciascuna area organizzativa omogenea.

Per la gestione documentale l'Amministrazione è tenuta ad utilizzare gli strumenti individuati dal Codice dell'Amministrazione Digitale, nel rispetto di quanto previsto dalle regole tecniche dettate con il DPCM 3 dicembre 2013.

Il sistema di gestione documentale, di cui il protocollo informatico è una delle componenti, deve prevedere l'uso degli strumenti digitali per la gestione dell'attività amministrativa dell'ente e deve inoltre garantire la sicurezza e l'integrità del sistema stesso.

Il sistema deve, inoltre, consentire il reperimento delle informazioni riguardanti i documenti registrati e l'accesso alle informazioni del sistema da parte dei soggetti interessati.

Per ciò che riguarda l'aspetto organizzativo, le amministrazioni sono innanzitutto tenute ad individuare le aree organizzative omogenee ed i relativi uffici e nominare per ciascuna di esse un Responsabile della gestione documentale. Se vi sono amministrazioni con più aree organizzative omogenee vi è l'obbligo di nominare il Coordinatore della gestione documentale.

Le amministrazioni, inoltre, hanno l'obbligo di redigere appositi manuali di procedura e di definire i tempi, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore e di reparto e, più in generale, dei protocolli diversi dal protocollo informatico.

Le Aree Organizzative Omogenee rappresentano, nelle intenzioni del legislatore, il punto di riferimento della gestione del flusso documentale.

Per Area Organizzativa Omogenea si intende un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato.

Secondo la normativa vigente, tutte le pubbliche amministrazioni sono tenute ad identificare le Aree Organizzative Omogenee assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.

Nel caso degli istituti scolastici, sarà individuata un'unica area organizzativa omogenea.

5.3 I soggetti coinvolti nella gestione documentale

Il responsabile della gestione documentale è il dirigente o il funzionario in possesso di requisiti professionali o di professionalità tecnico archivistica, dedicato al servizio per la tenuta del protocollo informatico, del workflow documentale e degli archivi. È necessario che il responsabile della gestione documentale abbia un vicario per i casi di assenza e/o impedimento a svolgere le sue funzioni.

Spetta al responsabile della gestione, dopo aver censito le esigenze dell'amministrazione in materia di gestione documentale, predisporre lo schema di manuale di gestione e dettare le procedure per la formazione dei documenti informatici, nonché per la tenuta dei fascicoli e per il flusso di lavorazione.

Il responsabile della gestione dovrà altresì redigere il piano per la sicurezza informatica dei documenti.

All'interno del sistema di gestione documentale, i singoli documenti sono organizzati per "fascicoli informatici" in cui raccogliere gli atti, i documenti e i dati relativi ad un determinato procedimento o a un determinato affare; nella pratica il fascicolo informatico è un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali allo svolgimento di una specifica attività o di uno specifico procedimento.

Sotto questo profilo, l'immaterialità del fascicolo digitale potrebbe creare alcuni problemi in materia di riservatezza dei dati dei soggetti coinvolti nel procedimento. Per questo motivo la Scuola deve adottare tutte le cautele necessarie a consentire che possano accedere ad un determinato fascicolo elettronico soltanto i dipendenti che si occupano di quello specifico affare, evitando la possibilità che altri - anche interni all'Ente - possano venire a conoscenza del contenuto del fascicolo medesimo.

Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale.

Per questo motivo, tutti i documenti dell'archivio devono essere organizzati secondo uno schema contenuto nel piano di classificazione.

Ad esempio, andranno inseriti nel fascicolo informatico di procedimento: i documenti in arrivo, i documenti in partenza (con le relative minute) e i documenti interni (anche se non protocollati).

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

- ricevuto;
- inviato;
- di rilevanza interna.

Nell'ambito del Manuale di gestione documentale, è possibile distinguere tra:

a) comunicazioni informali, che non hanno valenza giuridico probatoria né rilevanza ai fini dell'attività amministrativa;

b) scambio di documenti tra uffici di un certo rilievo ai fini dell'attività amministrativa.

Mentre per le prime è opportuno prevedere che possano essere inviate attraverso posta elettronica ordinaria e non siano soggette a protocollazione ed archiviazione, per i secondi è necessario prevedere che vengano archiviati e, in alcuni casi, possano essere protocollati.

5.4 Il Manuale della gestione documentale

Il Manuale di gestione documentale è uno dei documenti organizzativi più importanti per la vita dell'istituto: all'interno di questo, infatti, vengono indicati ruoli, procedure e strumenti per la gestione dei procedimenti amministrativi attraverso l'uso delle tecnologie info-telematiche.

All'interno del Manuale dovranno essere indicate:

a) a) le responsabilità connesse alla gestione dei documenti in entrata, in uscita ed interni alla stessa AOO

b) b) le modalità di interconnessione tra servizi di gestione documentale e di relazione con il pubblico, con particolare riguardo agli aspetti legati alla ricezione a mano dei documenti

Il Manuale di gestione è adottato con delibera dal Consiglio d'Istituto su proposta del Responsabile per la gestione documentale ed è pubblicato sul sito internet della scuola all'interno della sezione Amministrazione Trasparente.

Premessa al Modulo 6. L'importanza del protocollo informatico per l'efficienza degli uffici

Dal 1° gennaio 2004, è previsto che il protocollo delle Pubbliche Amministrazioni sia esclusivamente informatico.

Il Protocollo Informatico assicura maggior efficienza agli uffici pubblici, rispetto a quella del Registro di protocollo cartaceo. Già nel rapporto della Commissione Giannini del 1979, l'inefficienza dei sistemi connettivi (tra servizi di protocollo e archivi), veniva identificata come una delle maggiori carenze della Pubblica Amministrazione Italiana.

Il Protocollo informatico riesce a sopperire a tali inefficienze, poiché facilita l'identificazione dei documenti in archivio e li rende reperibili anche per un accesso esterno.

La normativa relativa al protocollo informatico, funge da garante dell'efficienza della funzione certificativa; assicurando che l'atto di protocollo sia un Atto Pubblico fide facente (atto di fede privilegiata), adatto a identificare i movimenti in entrata e uscita dei documenti relativi ad una determinata area organizzativa.

6 Il protocollo informatico

6.1 Introduzione

L'istituzione e la tenuta del protocollo informatico rappresenta uno dei primi obblighi a contenuto informatico che il legislatore ha posto per le amministrazioni italiane: la piena operatività del protocollo informatico, infatti, ben può essere ritenuta la chiave di volta del sistema normativo in materia di digitalizzazione dei procedimenti amministrativi.

In questo quadro, nel presente modulo, verrà innanzitutto descritta l'evoluzione normativa in materia di gestione del registro di protocollo da parte delle pubbliche amministrazioni e le finalità perseguite con l'introduzione del protocollo informatico.

Saranno poi descritti gli specifici obblighi incombenti sugli uffici in materia di tenuta del registro informatico di protocollo, anche alla luce delle regole tecniche dettate con il DPCM 3 dicembre 2013.

Infine, verranno illustrate le prescrizioni da rispettare con riferimento al registro di emergenza di protocollo nonché alle modalità di tenuta e conservazione del registro giornaliero di protocollo.

6.2 Il registro di protocollo informatico

Le attività di gestione dei documenti e degli archivi delle Pubbliche Amministrazioni, unitamente a quelle di protocollazione, rientrano tra i cd. "servizi di connettivo", vero e proprio punto nevralgico di ogni attività amministrativa. In particolare, l'attività di protocollazione è quella in cui si certifica mittente e destinatario di ogni comunicazione in entrata e in uscita, identificandola in maniera univoca nell'ambito di una sequenza numerica collegata con l'indicazione cronologica.

Il protocollo è un servizio obbligatorio delle pubbliche amministrazioni che ha la funzione di gestire, sia in entrata che in uscita dall'organizzazione, tutte le scritture e documenti.

È uno strumento dal duplice valore, giuridico-probatorio e gestionale. Sotto il primo profilo, sul registro di protocollo vengono trascritti progressivamente i documenti e gli atti in entrata e in uscita di un ufficio pubblico, attribuendo certezza ai momenti di arrivo/spedizione degli stessi; il valore gestionale, invece, è determinato dall'attività di classificazione del documento che consente il suo inserimento nel contesto del procedimento e quindi in relazione con i documenti correlati.

Il protocollo e la gestione dei flussi documentali hanno lo scopo primario di garantire il collegamento tra ciascun documento ricevuto dall'Amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali.

Attraverso il protocollo i documenti amministrativi, ricevuti o adottati, ricevono un'esatta e univoca identificazione. In questo modo, anche il cittadino ottiene la certezza che i documenti da lui prodotti siano stati acquisiti e registrati.

Questo servizio ha inoltre il compito di organizzare la memoria dell'Ente, mediante la classificazione degli atti protocollati secondo un ordinamento logico basato sulle funzioni e sulle attività dell'Amministrazione.

Per assolvere queste funzioni, il protocollo è:

a) **un atto pubblico:** colui che lo redige deve essere un pubblico ufficiale;

b) **un atto di "fede pubblica":** utilizzabile, oltre che per evenienze pratiche e amministrative, anche per qualsiasi necessità probatoria;

c) **un atto di "fede privilegiata":** fa piena prova fino a querela di falso.

L'introduzione delle tecnologie informatiche, comportando quella che è stata definita "smaterializzazione del documento", richiedeva un intervento legislativo al fine di garantire che il sistema informatico di gestione dei flussi documentali fornisse le stesse certezze (in termini di autenticità) e la stessa affidabilità (in termini di fede privilegiata) di quello tradizionale. Infatti, la disciplina dell'organizzazione dei pubblici uffici, nonché il regime giuridico della loro attività, era stata dettata con esclusivo riferimento ai tradizionali concetti di documento (cartaceo) e firma (autografa).

Il protocollo informatico, in base all'art. 50 DPR 445/2000, sostituisce il tradizionale protocollo cartaceo a far data dal 1° gennaio 2004.

Il legislatore definisce protocollo informatizzato (indicato anche come protocollo informatico) come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dalle amministrazioni per la gestione dei documenti", ovvero, tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali.

Grazie al protocollo informatico diviene possibile registrare in maniera automatizzata le informazioni di protocollo di ogni documento ricevuto o spedito dall'Amministrazione.

L'introduzione di questo istituto risponde alla necessità di eliminare i registri cartacei, diminuire gli uffici di protocollo e migliorare il flusso informativo e documentale degli uffici, anche ai fini di snellimento e trasparenza dell'azione amministrativa.

La normativa in materia di protocollo informatico risponde ad un triplice ordine di ragioni:

a) i sistemi di protocollo informatico, oltre ad essere orientati alla trasparenza amministrativa e finalizzati ad accrescere l'efficienza interna, devono continuare a garantire, seppure in nuova forma, la funzione certificativa tipica dell'attività di protocollazione;

b) oltre a comportare un contenimento dei costi, dovrebbe rappresentare anche un fattore di razionalizzazione dell'attività amministrativa. Ciò si realizza attraverso l'eliminazione dei registri cartacei con il conseguente recupero delle risorse umane, materiali e finanziarie finora utilizzate per la protocollazione tradizionale e la riduzione degli uffici di protocollo;

c) l'adozione del protocollo informatico persegue anche il fine di migliorare la trasparenza dell'azione amministrativa attraverso l'uso di dispositivi che rendano effettivo il diritto di accesso di imprese e cittadini allo stato dei procedimenti in cui sono interessati ed alla visione dei relativi documenti.

In ciascuna Area Organizzativa Omogenea il registro informatico di protocollo deve essere unico sia per la protocollazione in ingresso che in uscita.

La numerazione, progressiva, si chiude al 31 dicembre e inizia il 1° gennaio successivo.

In conformità alla normativa vigente, nel Manuale di gestione documentale dell'Amministrazione sono indicati i tempi, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, e, più in generale, dei protocolli diversi dal protocollo informatico.

La preferenza che il legislatore accorda al Registro di protocollo informatico è conseguenza della circostanza per cui, dal punto di vista tecnico, il protocollo informatico – al contrario degli altri registri - deve necessariamente essere sviluppato in modo da fornire le stesse garanzie di certezza ed affidabilità che contraddistinguevano il registro cartaceo e che consentano di assicurare immodificabilità e fede giuridica privilegiata anche alle attestazioni del protocollo informatico.

Il sistema informativo deve altresì presentare una serie di requisiti minimi di sicurezza al fine di salvaguardare l'integrità e la riservatezza dei dati ivi memorizzati.

Le modalità di tenuta del registro di protocollo informatico sono definite con Regole tecniche adottate con DPCM 3 dicembre 2013, che definisce gli specifici adempimenti tecnologici ed organizzativi che le amministrazioni devono compiere per tenere un registro di protocollo che mantenga inalterata la propria fede pubblica privilegiata.

Quest'ultima, infatti, è diretta conseguenza – da parte dell'amministrazione – del rispetto tassativo delle regole contenute nel Testo Unico sulla Documentazione Amministrativa (DPR n. 445/2000), nelle regole tecniche (DPCM 3 dicembre 2013) nonché delle cautele esplicitate all'interno del Manuale per la gestione dei flussi documentali.

6.3 Adempimenti in materia di protocollo informatico

Il sistema di protocollo informatico deve garantire le funzionalità minime, ovvero quelle che permettono di fornire il servizio di certificazione. Tali funzionalità prevedono:

- la registrazione in un archivio informatico delle informazioni riguardanti il documento in entrata o in uscita;
- la segnatura, consistente nell'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
- l'adozione di un titolario di classificazione per permettere all'Amministrazione di archiviare i documenti protocollati a seconda della funzione o attività cui essi fanno riferimento.

In tal modo, oltre a favorire la ricerca dei documenti protocollati, che comunque può avvenire anche mediante l'uso di parole chiave, si pongono le basi per una concreta gestione dell'intero patrimonio documentale dell'Amministrazione.

La soluzione informatica di protocollo adottata dall'amministrazione garantisce il rispetto dei requisiti tecnici prescritti dalla normativa vigente.

Ma l'avvio di un programma di informatizzazione del protocollo che si estende all'automazione dei processi e delle funzioni di gestione documentale non può essere ridotto ad una questione di introduzione di tecnologia.

Al contrario l'introduzione dei nuovi strumenti tecnologici può portare ai risultati finali attesi solo se coniugata ad un intervento organizzativo di grande profondità. Per questo motivo, gli utenti sono tenuti al rispetto delle regole adottate e, in particolare, del Manuale della gestione documentale che deve essere adottato da ogni scuola e pubblicato sul sito istituzionale.

Con l'operazione di registrazione di protocollo vengono memorizzati in archivio tutti i dati che contraddistinguono in modo univoco i documenti ricevuti o spediti dall'Amministrazione.

Per esigenze di sicurezza, e al fine di tutelare la integrità dei dati dell'archivio, le operazioni di modifica causate da eventuali errori devono avvenire in modo trasparente.

Le regole per la corretta scrittura dei dati di protocollo sono contenute all'interno del Manuale per la Gestione dei flussi documentali.

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Amministrazione e tutti i documenti informatici.

Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della Pubblica Amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'Amministrazione così come individuati nel Manuale per la gestione dei flussi documentali.

L'operazione di segnatura risponde all'esigenza di identificare ogni documento protocollato in modo inequivocabile. La segnatura consiste nell'apposizione o associazione al documento (cartaceo o informatico) delle informazioni ad esso relative.

La segnatura è effettuata automaticamente e contemporaneamente alla registrazione di protocollo.

Per quanto riguarda i documenti cartacei, l'operazione di acquisizione è possibile solo dopo che la segnatura è stata acquisita sull'originale cartaceo, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Le operazioni di annullamento e modifica delle informazioni inserite nella fase di registrazione devono avvenire in modo che ne rimanga traccia.

L'annullamento delle informazioni registrate in forma non modificabile comporta l'annullamento di tutta la registrazione. In caso di annullamento di altre informazioni, si renderà necessaria solo la rinnovazione del campo interessato. In questo caso deve essere contestualmente memorizzato, in modo permanente, il valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.

In caso di malfunzionamento della procedura informatizzata del protocollo, il responsabile del servizio deve autorizzare la procedura di emergenza.

Ogni qualvolta, per cause tecniche, non sia possibile utilizzare la procedura informatica, le operazioni di protocollatura vengono svolte, eventualmente anche in forma cartacea, sul registro di emergenza.

Sul registro sono riportate la causa, la data e l'ora di inizio dell'interruzione. Terminata l'emergenza, tutte le registrazioni devono essere opportunamente riportate nel protocollo informatico. È buona norma che il registro di emergenza sia già predisposto e conservato dal responsabile del servizio.

Il registro di emergenza viene rinnovato ogni anno solare. Qualora nel corso dell'anno il registro di emergenza non venisse utilizzato, il responsabile del servizio annoterà su di esso il mancato uso.

Le registrazioni effettuate sul protocollo di emergenza sono equivalenti a quelle eseguite sul registro di protocollo generale.

6.4 Registro giornaliero di protocollo informatico

Il legislatore prescrive la tenuta anche di un registro giornaliero di protocollo.

Il registro giornaliero deve contenere, in modo ordinato e progressivo, l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Il documento informatico "Registro giornaliero di protocollo" deve quindi possedere tre caratteristiche:

- staticità;
- immodificabilità;

- integrità.

Il registro giornaliero di protocollo viene validamente formato mediante la produzione di una semplice estrazione statica dei dati contenuti nel Sistema di gestione informatica del protocollo dell'Amministrazione con la quale è possibile ottenere (quale risultato dell'estrazione) un documento informatico.

Una volta generato e reso immodificabile, il registro giornaliero deve essere inviato al sistema di conservazione entro la giornata lavorativa successiva.

Premessa al Modulo 7. La validità legale dei documenti informatici nel tempo

Negli archivi delle Pubbliche amministrazioni, vi è la certezza delle situazioni giuridiche, delle situazioni patrimoniali e, in generale, delle informazioni sulle persone dal conseguimento di un determinato titolo di studio allo stato civile.

È necessario quindi, che l'affidabilità di questa documentazione sia garantita anche nella la transizione dal cartaceo al digitale.

Per tale motivazione il legislatore ha promosso all'interno di ogni amministrazione un sistema di conservazione di documenti informatici, che ne garantisca nel tempo la conservazione e l'integrità a livello legale. Per questo motivo tutte le amministrazioni sono chiamate a questo necessario adeguamento, che assicuri al sistema di conservazione e ai documenti:

- La certificazione della provenienza;
- L'integrità. La garanzia che il documento non sia stato modificato nel corso del tempo;
- La disponibilità e l'accessibilità. La garanzia che il documento possa essere ricercato e visionato;
- La sicurezza. Necessaria per proteggere i dati personali dei cittadini contenuti negli archivi.

Il Sistema di Conservazione dei Documenti Informatici, è uno dei più complessi adempimenti richiesti alle amministrazioni, poiché protegge i dati sulle attività degli enti, la certezza delle situazioni giuridiche e – perché no - la memoria storica di tutto il Paese.

7 Il sistema di conservazione dei documenti informatici

7.1 Introduzione

Il Codice dell'Amministrazione Digitale obbliga le Pubbliche Amministrazioni ad attuare interventi specifici volti ad istituire e regolamentare un sistema di conservazione dei documenti informatici che abbia la finalità di assicurare che gli archivi pubblici conservino nel tempo la loro integrità e affidabilità.

In questo quadro, il CAD contiene indicazioni chiare sulla conservazione nel tempo dei documenti digitali, ponendo una condizione essenziale per rendere effettivo il passaggio dalla carta al digitale.

Nel corso del presente modulo, dopo l'illustrazione delle caratteristiche del sistema di conservazione documentale, vengono evidenziate le diverse figure coinvolte nel processo di conservazione ed i rispettivi ruoli.

In particolare, vengono descritte la figura e il ruolo del responsabile della conservazione documentale e dei conservatori esterni, definendone i rispettivi ambiti di attività.

Infine, viene illustrato il contenuto del Manuale di conservazione documentale che deve essere obbligatoriamente adottato da tutte le pubbliche amministrazioni, conformemente a quanto previsto nelle regole tecniche adottate con DPCM 3 dicembre 2013.

7.2 La conservazione nel tempo dei documenti informatici

Come qualunque documento, anche quelli informatici sono soggetti ad un progressivo e inevitabile processo di obsolescenza che provoca gravi rischi di manipolazioni e perdita di informazione.

La formalizzazione dei concetti e dei principi connessi alla "conservazione" delle risorse digitali ha polarizzato l'attenzione della comunità scientifica (in particolare del mondo archivistico) negli ultimi anni, con particolare riguardo ai nodi concettuali, ai vincoli e alle criticità di tipo organizzativo, alla revisione della normativa, allo studio della tipologia dei formati e dei metodi per la conservazione.

Le logiche e le prassi legate alla funzione conservativa delle memorie digitali comportano un significativo cambiamento rispetto alle pratiche tradizionali legate alla documentazione cartacea: una delle caratteristiche precipue della conservazione in ambiente digitale è infatti una funzione attiva e continua nel tempo.

La conservazione può essere definita come l'insieme delle attività finalizzate a garantire nel tempo la validità legale di un documento informatico.

Attraverso un processo di conservazione rispettoso della normativa di settore in materia, le Pubbliche Amministrazioni sono in grado di mantenere inalterate nel tempo le caratteristiche di integrità, accessibilità, leggibilità e riproducibilità, unitamente alla capacità di dimostrare l'autenticità del documento informatico.

L'art. 44 CAD prescrive a tutte le Pubbliche Amministrazioni di istituire un sistema di conservazione dei documenti informatici in grado di assicurare:

a) l'identificazione certa del soggetto che ha formato il documento e dell'Amministrazione o dell'area organizzativa omogenea di riferimento;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196 (Codice Privacy).

Con DPCM 3 dicembre 2013 sono state adottate le nuove Regole tecniche per la conservazione dei documenti informatici .

Tali regole sostituiscono le precedenti regole dettate dalla deliberazione CNIPA n. 11 del 2004.

I sistemi di conservazione già esistenti dovranno adeguarsi alle nuove regole entro 36 mesi dall'entrata in vigore del decreto (11 aprile 2017) secondo un piano dettagliato da allegare al manuale della conservazione (documento che, come si vedrà, è obbligatorio anche per le scuole). I lotti di documenti conservati fino ad oggi (e nei successivi giorni necessari ad aggiornare i sistemi) potranno (la scelta spetta al Responsabile della conservazione interno alla struttura che ha l'obbligo di conservazione) continuare ad essere conservati con le precedenti regole tecniche o potranno essere riversati nel nuovo sistema di conservazione.

La conservazione dei documenti informatici può essere svolta in base a due distinti modelli:

a) c.d. conservazione interna: il processo è svolto all'interno della struttura che ha prodotto o detiene i documenti informatici da conservare;

b) c.d. conservazione esterna: il processo è affidato, del tutto o in parte, ad altri soggetti (pubblici o privati) che offrono idonee garanzie organizzative e tecnologiche.

Nell'ambito del sistema di Conservazione vengono individuati almeno tre ruoli:

- **il produttore:** persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale;

- l'**utente:** persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse (es. richiedente accesso atti ai sensi della Legge 241/1990 o autorità giudiziaria che abbia bisogno di acquisire documenti dal produttore);
- **il responsabile della Conservazione:** è la persona fisica che definisce e gestisce il sistema di Conservazione in relazione al modello organizzativo adottato e definito dal manuale della Conservazione.

Il sistema di conservazione assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;

b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Vale la pena di ricordare che, in base al DPCM 13 novembre 2014, sono documenti informatici:

- documenti di testo, fogli di calcolo, schemi XML redatti tramite l'utilizzo di appositi strumenti software;
- documenti acquisiti per via telematica o su supporto informatico, e-mail, documenti acquisiti come copia per immagine di un documento analogico;
- registrazioni informatiche di transazioni o processi informatici, dati forniti dall'utente attraverso la compilazione di moduli o formulari elettronici;
- insieme di dati, provenienti da una o più basi dati, raggruppati secondo una struttura logica determinata (viste).

Elementi fondamentali di un sistema di conservazione, i pacchetti informativi sono i veri e propri oggetti della conservazione. A seconda delle funzioni che devono svolgere, esistono vari tipi di pacchetti informativi previsti dalle regole tecniche:

- **pacchetto di versamento:** questa tipologia di pacchetto è il documento inviato a un sistema di conservazione dal Produttore. È l'insieme dei dati sottoposti al sistema di conservazione. Il dettaglio dei contenuti di tale documento è frutto di un accordo tra il Produttore e il Conservatore;
- **pacchetto di archiviazione:** è un derivato del pacchetto di versamento o di più pacchetti di versamento. Attraverso di esso vengono trasmessi al sistema di conservazione;
- **pacchetto di distribuzione:** è il pacchetto inviato a un Utente dal sistema di conservazione a seguito dell'interrogazione del sistema.

7.3 Il Responsabile della conservazione

Diversi sono i ruoli coinvolti nell'ambito del sistema di conservazione documentale.

Lo stesso art. 44 CAD prevede, infatti, che il sistema debba essere gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali e, ove esistente, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, nella definizione e gestione delle attività di rispettiva competenza**.**

Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

Tali soggetti prendono il nome di Conservatori.

Il Responsabile della conservazione:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, ovviarvi; adotta analoghe misure riguardo l'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia previsto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico e in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il responsabile della conservazione è sempre figura interna all'Amministrazione che può coincidere con il responsabile della gestione documentale.

È logico ritenere che la responsabilità della conservazione debba essere affidata ad una figura professionale dotata di idonee conoscenze in materia di:

- archivistica, perché si tratta di garantire la formazione, conservazione e fruizione di archivi digitali;
- informatica, per fare le giuste scelte relativamente ai supporti di memorizzazione, ai formati elettronici, al sistema di conservazione digitale;
- diritto e diplomatica del documento contemporaneo, per avere la capacità di valutare l'autenticità, gli elementi intrinseci ed estrinseci, l'accessibilità, l'intelligibilità e la riproducibilità dei documenti informatici;
- organizzazione, in quanto la produzione dei documenti informatici comporta necessariamente la rimodulazione degli assetti organizzativi e il reengineering dei processi operativi.

Come anticipato, i conservatori esterni sono i soggetti (pubblici o privati) ai quali il responsabile della conservazione può delegare tutto o parte del processo di conservazione.

L'attività di conservatore può essere svolta senza la necessità di ottenere preventivamente alcun permesso o autorizzazione.

Tuttavia, il legislatore ha previsto la possibilità per i conservatori più professionali di ottenere un apposito "accreditamento", rilasciato dall'Agenzia per l'Italia Digitale, quale riconoscimento del più elevato livello di professionalità.

È importante osservare come le pubbliche amministrazioni possano rivolgersi solo a conservatori accreditati.

I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso l'Agenzia per l'Italia Digitale.

Con la Circolare n. 65/2014 AgID ha ridefinito le modalità per l'accreditamento e per la vigilanza dei soggetti che intendono conseguire i riconoscimenti più elevati in termini di qualità e sicurezza prevedendone l'iscrizione in un apposito elenco pubblico (disponibile all'indirizzo http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi).

La circolare si sofferma sui requisiti per l'accreditamento dei conservatori, sulle modalità di presentazione della domanda e sul correlato iter istruttorio, dettando anche le linee guida per la vigilanza.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate.

Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato.

In ogni caso deve essere previsto per il conservatore esterno l'obbligo di rispettare il manuale di conservazione predisposto dal responsabile dell'Amministrazione.

Il soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali.

7.4 Il manuale della conservazione

Il sistema di Conservazione, le tipologie di documenti conservati, i processi e tutti i ruoli che intervengono nella Conservazione Digitale sono dettagliatamente descritti e identificati nel manuale di Conservazione.

Gli obiettivi del manuale, nello specifico, sono i seguenti:

- descrizione dei ruoli, delle competenze e delle responsabilità dei ruoli coinvolti nel processo di Conservazione;
- descrizione dei processi di gestione dei documenti caricati nel sistema di Conservazione;
- definizione degli aspetti tecnici dei documenti recepibili e dei documenti generati nelle varie fasi del processo di Conservazione;
- descrizione del processo di firma e verifica dei documenti da parte del Responsabile;
- definizione delle attività di monitoraggio e controllo;
- individuazione delle attività necessarie al fine di adempiere agli obblighi di esibizione dei documenti.

Il processo di conservazione consta di più fasi e, in particolare:

a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;

b) la verifica che il pacchetto di versamento sia coerente con le modalità previste dal manuale di conservazione (con rifiuto nel caso in cui le verifiche abbiano evidenziato anomalie);

c) la generazione del rapporto di versamento relativo ad uno o più pacchetti di versamento (tale rapporto può essere sottoscritto con firma digitale o qualificata);

d) la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e la gestione del pacchetto di archiviazione;

e) la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

f) lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore. Naturalmente, nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene, previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo, rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono.

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura;

2. sicurezza;

3. portabilità;

4. funzionalità;

5. supporto allo sviluppo;

6. diffusione.

I formati utilizzati dall'Amministrazione sono tassativamente indicati all'interno del Manuale di gestione documentale e del Manuale di conservazione dei documenti informatici.

Premessa al Modulo 8. La sicurezza dei documenti informatici

Non può esistere amministrazione digitale, senza sicurezza informatica.

Il fondamento dell'attività amministrativa digitale è necessariamente la sicurezza, intesa come predisposizione di tutte le cautele tecnologiche e organizzative, per assicurare i requisiti di integrità, affidabilità e disponibilità, a chi ne ha titolo, di quanto contenuto negli archivi.

L'Amministrazione deve presidiare i vari rischi in cui possono incorrere i documenti conservati, ad esempio di perdita accidentale, di accesso e/o modifica non autorizzati.

Il legislatore, dati gli elevati livelli di protezione richiesti, ha attivato molte disposizioni a tutela degli archivi, con la necessità di un adeguato numero di operatori coinvolti nella sicurezza informatica.

Ad esempio, soggetti come:

- Il Responsabile per il trattamento dei dati personali;
- Il Responsabile per la sicurezza dell'amministrazione;
- Il Responsabile e il coordinatore della gestione documentale;
- Il Responsabile della conservazione dei documenti informatici,

adottano e inseriscono nei manuali di rispettiva competenza, delle cautele di sicurezza, che tutti i dipendenti devono adottare per conservare integrità e riservatezza dei documenti che generano, o che sono custoditi negli archivi dell'Amministrazione.

8 La sicurezza dei documenti

8.1 Introduzione

Alla luce del sempre maggiore utilizzo delle nuove tecnologie per la gestione dei procedimenti amministrativi, l'Amministrazione è chiamata ad organizzarsi e pianificare le iniziative necessarie tese a salvaguardare l'integrità e la disponibilità delle informazioni trattate, nonché la confidenzialità delle stesse.

Quando i dati, le informazioni e le applicazioni che li trattano sono parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali dell'ente, diventano un bene primario cui è necessario garantire salvaguardia e disponibilità; essendo la disponibilità uno dei cardini della sicurezza, unitamente a confidenzialità ed integrità, la disciplina normativa in materia di sicurezza rappresenta parte integrante dei procedimenti amministrativi.

Nel corso del presente modulo formativo, dopo una prima introduzione alla nozione di sicurezza informatica, saranno illustrate le principali normative in materia dettate dal Codice Privacy, dal Codice dell'Amministrazione Digitale e dalle relative regole tecniche.

Infine, verrà affrontato il tema della continuità operativa e del *disaster recovery* e degli adempimenti vigenti per le pubbliche amministrazioni.

8.2 L'importanza della sicurezza informatica

Il Codice dell'Amministrazione Digitale contiene l'obbligo per gli uffici pubblici di utilizzare le nuove tecnologie per la gestione dei procedimenti amministrativi e l'erogazione di servizi a cittadini e imprese.

Conseguentemente - e con l'obiettivo di creare una PA efficiente, rapida e sicura - il legislatore si è occupato di fornire precise indicazioni anche in merito alla sicurezza dei nuovi sistemi, per ridurre al minimo i rischi di perdita di dati o di default del sistema.

Il problema della sicurezza è uno dei gangli principali di tutti i sistemi informativi ma, se possibile, è ancora più importante nel settore pubblico. Le Pubbliche Amministrazioni nell'esercizio della propria attività istituzionale raccolgono, producono ed archiviano un'enorme quantità di dati e documenti. In base alle norme fin qui esaminate, tutte queste informazioni dovranno essere rese disponibili "in modalità digitale". Questo significa che i dati dovranno essere formati, acquisiti e conservati nei sistemi informatici delle Amministrazioni titolari.

Si tratta di un vero e proprio patrimonio che deve essere tutelato per:

a) mantenere l'integrità, e quindi l'affidabilità, delle informazioni pubbliche;

b) prevenire e limitare i danni da intrusioni e accessi abusivi;

c) evitare possibilità di diffusioni non autorizzate di informazioni;

d) consentire un corretto funzionamento dell'apparato burocratico ed evitare la perdita del valore probatorio di documenti e registri.

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente.

Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurare l'integrità, la riservatezza e la disponibilità delle informazioni archiviate nei sistemi informatici.

I vantaggi e le opportunità offerte dall'uso delle tecnologie info-telematiche sono assai rilevanti, soprattutto in termini di riduzione dei costi e incremento di efficienza; tuttavia, bisogna anche tenere conto le criticità rappresentate dalle vulnerabilità dei sistemi informatici.

Sotto questo profilo, assume centrale importanza la sicurezza informatica, intesa come complesso di tutte le operazioni e accorgimenti adottati al fine di rendere vani i tentativi di attacchi (passivi ed attivi) che possono essere perpetrati ai danni di un sistema informatico.

Garantire la sicurezza informatica di un sistema significa:

- garantire che i dati e i documenti siano integri e aggiornati;
- garantire che i dati e i documenti siano protetti da accessi non autorizzati;
- garantire che i dati e i documenti siano facilmente disponibili agli utenti autorizzati.

Lo stesso concetto di Pubblica Amministrazione Digitale si fonda sul necessario ed implicito presupposto che siano sicuri i sistemi informatici usati dagli uffici pubblici.

Tale sicurezza serve a preservare l'integrità e immodificabilità dei documenti e degli archivi della Pubblica Amministrazione.

Infatti, la sicurezza di questi ultimi è necessaria per garantire la correttezza delle scelte dell'Amministrazione e per conservare la fede pubblica privilegiata degli atti dell'ente.

La crescente complessità delle attività legate alla Pubblica Amministrazione, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio, quali quelli determinati da un attacco di tipo terroristico o anche solamente malevolo, così come gli inconvenienti di natura tecnica, che possono portare all'interruzione totale dei servizi istituzionali anche per lunghi periodi, evidenziano l'esigenza che le amministrazioni si occupino costantemente della sicurezza dei propri sistemi, in modo da poter sempre garantire la propria operatività.

8.3 Gli obblighi normativi in materia di sicurezza informatica

Le norme in materia di digitalizzazione dell'attività amministrativa hanno determinato la necessaria transizione da una PA tradizionale ad una PA digitale, spingendo gli uffici ad affrontare (e risolvere) le problematiche legate alla sicurezza.

Proprio allo scopo di accompagnare le amministrazioni in questo processo, il legislatore ha dettato numerose disposizioni in materia di sicurezza, riservatezza e continuità operativa; tali previsioni rappresentano una vera e propria checklist che tutte le amministrazioni devono seguire.

La gran parte di queste norme, lungi dall'affermare disposizioni meramente di principio, impone alle Amministrazioni obblighi precisi in ordine alle misure da adottare per assicurare la sicurezza dei propri sistemi e, quindi, dei propri dati.

Il legislatore non si preoccupa di imporre l'utilizzo di specifiche tecnologie, ma – piuttosto – prevede veri e propri obblighi di tipo organizzativo che hanno la finalità di assicurare che le amministrazioni adottino tutte le cautele più opportune.

La centralità del tema della sicurezza dei sistemi informativi delle Pubbliche Amministrazioni, e quindi dei dati in esse contenuti, trova conferma nell'art. 51 del Codice dell'Amministrazione Digitale.

È importante sottolineare come in tale norma siano indicati i principi cui devono essere improntati i sistemi informativi delle Amministrazioni:

a) **integrità ed esattezza dei dati.** I dati custoditi nei sistemi devono essere modificati o eliminati solo dai soggetti all'uopo abilitati; è quindi necessario che il sistema sia congegnato in modo tale da prevedere diversi livelli di autenticazione e consentire comunque che rimanga traccia delle diverse operazioni svolte;

b) **disponibilità e accessibilità.** I dati devono poter essere fruibili alle Amministrazioni e ai cittadini che ne abbiano diritto;

c) **riservatezza e confidenzialità.** Il sistema deve essere strutturato in modo da evitare il rischio di accessi non autorizzati.

Numerose disposizioni in materia di sicurezza sono inoltre contenute anche nelle diverse regole tecniche adottate in base al CAD: dalle regole tecniche sul protocollo informatico a quelle in materia di conservazione, da quelle sulle firme elettroniche a quelle sul documento informatico.

I documenti informatici delle Pubbliche Amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

Deve altresì essere garantita costantemente l'immodificabilità dei documenti e degli archivi in cui questi sono custoditi.

Evidente la finalità delle norme: ridurre i rischi che possono derivare da atti dolosi (ad es. sabotaggi o accessi abusivi) o da eventi accidentali (come errori compiuti dal personale o eventi calamitosi).

Il Codice dell'Amministrazione Digitale rinvia ad apposite regole tecniche in merito alle misure necessarie a garantire la sicurezza del sistema di gestione documentale.

In materia, il DPCM 3 dicembre 2013, nel dettare le norme in materia, prescrive innanzitutto i requisiti che deve possedere il sistema di protocollo informatico.

Si tratta, in particolare:

- dell'univoca identificazione ed autenticazione degli utenti;
- della protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- della garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- della garanzia della registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Le regole tecniche, inoltre, prescrivono all'amministrazione di adottare – nell'ambito del manuale di gestione del sistema – un apposito piano di sicurezza relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici.

Tale documento è allegato al Manuale di gestione predisposto dal Coordinatore della gestione documentale.

In modo analogo a quanto previsto per il sistema di gestione documentale, il DPCM 3 dicembre 2013 prevede apposite disposizioni finalizzate a garantire la sicurezza del sistema di conservazione documentale e, quindi, l'integrità nel tempo dei documenti ivi memorizzati.

In particolare, è previsto che – nell'ambito del manuale per la conservazione – venga predisposto un apposito piano per la sicurezza che debba essere predisposto di concerto con il responsabile per la sicurezza e coordinandolo con gli altri documenti redatti dall'Amministrazione.

Non si può non evidenziare la rilevanza strategica che assume l'adozione delle cautele di sicurezza, considerando che il Codice dell'Amministrazione Digitale impone alle Amministrazioni di attivarsi per il rispetto delle regole tecniche sulle modalità di formazione, tenuta, conservazione e gestione del documento informatico e dei flussi documentali.

Numerose disposizioni, infatti, fanno espresso riferimento alla circostanza per cui l'efficacia giuridica e il valore probatorio di un documento informatico dipendono anche dalle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Si ritiene opportuno evidenziare che quelle contenute nel CAD non sono le uniche norme in materia di sicurezza informatica dei sistemi informativi delle Amministrazioni. Sul tema della sicurezza informatica nel settore pubblico insistono già molteplici provvedimenti (leggi, direttive, circolari).

In particolare, deve essere tenuta in debita considerazione la disciplina in materia di riservatezza dei dati personali (che è richiamata più volte dal CAD e dalle regole tecniche): il Codice privacy, infatti, prevede una serie di obblighi di sicurezza per tutti i soggetti, pubblici come privati, che compiano operazioni di trattamento dei dati personali.

La normativa sulla privacy da un lato impone un elenco di misure minime che devono essere adottate da ogni titolare, dall'altro impone ai titolari di proteggere i dati personali trattati in relazione alla natura del trattamento effettuato, alla tipologia dei dati stessi e coerentemente con le tecnologie disponibili, senza che siano indicati elementi limitanti rispetto a tale responsabilità.

Si tratta dunque di due aspetti - misure minime e misure idonee e preventive - di cui ogni Ente deve farsi carico congiuntamente. Le prime per evitare sanzioni penali e amministrative, le seconde per evitare responsabilità civili.

L'articolo 31 D. Lgs. n. 196/2003 impone al titolare del trattamento di predisporre tutte le misure di sicurezza idonee a ridurre al minimo "i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

In relazione all'art. 31, la normativa non prevede misure specifiche né potrebbe farlo, considerando la peculiarità di ciascun contesto: di conseguenza, l'individuazione delle misure idonee deve quindi essere ricondotta al processo generale di valutazione dei rischi, facendo riferimento:

- al tipo di dati trattati;
- al tipo di tecnologie utilizzate.

Nel quadro dei più generali obblighi di sicurezza contenuti del Codice Privacy, le Amministrazioni sono comunque tenute ad adottare le misure minime individuate dallo stesso Codice.

In particolare, le Amministrazioni sono tenute ad adottare le seguenti cautele:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale.

8.4 La continuità operativa e il *disaster recovery*

Il processo di digitalizzazione dell'azione amministrativa, per avere successo, richiede, tra l'altro, l'esistenza di un'infrastruttura informatica che risponda a particolari requisiti di efficienza e, quindi, di continuità, pena l'impossibilità per cittadini e imprese di accedere ai servizi delle amministrazioni.

Gli Enti sono quindi tenuti ad organizzarsi per assicurare la continuità nel funzionamento dell'organizzazione anche in modalità *digitale.*

L'art. 97 della Costituzione sancisce, infatti, un generale principio organizzativo di carattere programmatico che riguarda la Pubblica Amministrazione: gli uffici pubblici, infatti, devono essere organizzati in modo che siano garanti il buon funzionamento e l'imparzialità dell'Amministrazione.

Da tale principio consegue per il settore pubblico l'obbligo di assicurare la sicurezza di dati e documenti oltre alla continuità dei propri servizi: si tratta di due presupposti necessari a garantire da un lato la fiducia della collettività nella Pubblica Amministrazione e, dall'altro, per assicurare il corretto e regolare svolgimento della vita nel Paese.

La centrale importanza che i sistemi informatici di gestione e conservazione documentale rivestono per l'Amministrazione impone agli uffici di occuparsi di "*disaster recovery*"; con tale termine si intendono gli accorgimenti organizzativi e le soluzioni tecniche, organizzative e procedurali adottate per garantire il ripristino dello stato di un sistema Informatico (o di parte di esso), compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

Il Codice dell'Amministrazione Digitale rafforza ulteriormente il quadro giuridico relativo alla corretta formazione, raccolta e conservazione di documenti, al fine di garantire la costante operatività dei sistemi informativi quale presupposto fondamentale per la qualità e costante fruibilità dei dati, delle informazioni e dei servizi che le stesse PA rendono ai cittadini e alle imprese.

L'articolo 50-bis del CAD delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni in materia di continuità operativa.

In particolare, è previsto che tutte le amministrazioni tenute all'applicazione del CAD debbano predisporre piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività.

Nell'ambito della documentazione relativa alla sicurezza, tutte le amministrazioni definiscono pertanto un vero e proprio piano di continuità operativa e di *disaster recovery*.