ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
ANDREA TORRENTE

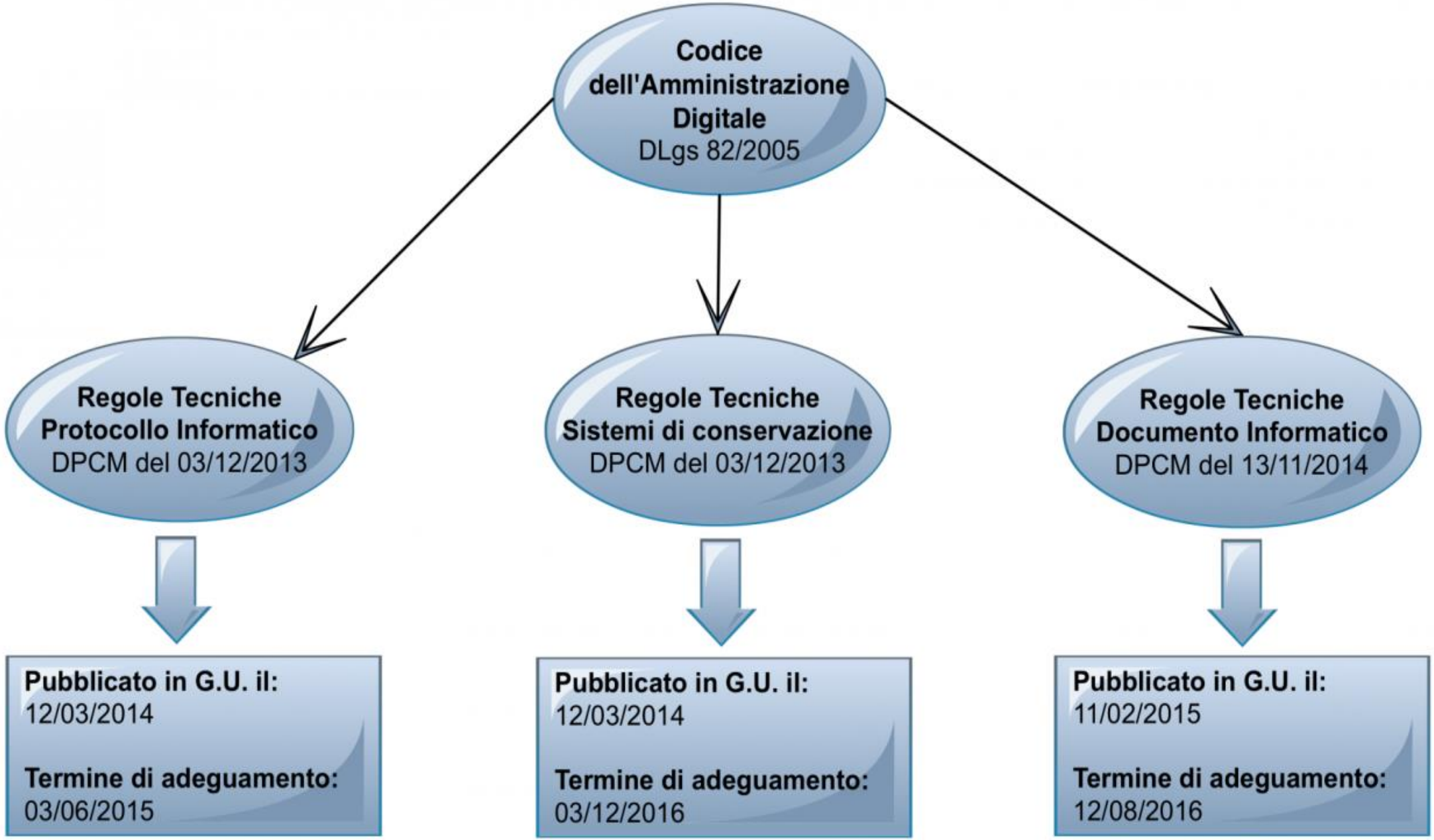
FORMAZIONE
DSGA
NEOASSUNTI
TEMATICA N.5

I Principi Dell'architettura Digitale della Scuola. La Digitalizzazione delle Procedure Amministrative e delle diverse Piattaforme Digitali del M.I.

Elaborazione & presentazione a cura di:
D.S.G.A. Loredana Mauriello

IL CODICE DELL' AMMINISTRAZIONE DIGITALE
D.LGS. 7 marzo 2005 n.82

Il D. Lgs 82/2005, entrato in vigore il 1° gennaio del 2006, regola e disciplina il processo di telematizzazione della Pubblica Amministrazione: la gestione, l'accesso, la trasmissione e la conservazione dei documenti digitali e tutto ciò che riguarda le comunicazioni telematiche tra le Pubbliche Amministrazioni, tra i privati e la Pubblica Amministrazione, finanche tra i privati stessi.


Codice dell'Amministrazione Digitale
DLgs 82/2005
Regole Tecniche Protocollo Informatico
DPCM del 03/12/2013
Regole Tecniche Sistemi di conservazione
DPCM del 03/12/2013
Regole Tecniche Documento Informatico
DPCM del 13/11/2014
Pubblicato in G.U. il:
12/03/2014
Termine di adeguamento:
03/06/2015
Pubblicato in G.U. il:
12/03/2014
Termine di adeguamento:
03/12/2016
Pubblicato in G.U. il:
11/02/2015
Termine di adeguamento:
12/08/2016

IL CODICE DELL' AMMINISTRAZIONE DIGITALE
D.LGS. 7 marzo 2005 n.82

Significativi aggiornamenti sono intervenuti con il D. Lgs. 235/2010, entrato in vigore il 25 gennaio 2011, che ha introdotto incentivi e sanzioni per il personale amministrativo, il diritto all'uso delle tecnologie, la coordinazione tra le amministrazioni, la possibilità di tesaurizzare i risparmi ottenuti con l'innovazione tecnologica.

IL CODICE DELL‘ AMMINISTRAZIONE DIGITALE
D.LGS. 7 marzo 2005 n.82

Il Codice dell'Amministrazione digitale è un testo unico che riunisce e riordina diverse norme, riorganizzando la materia delle informazioni e dei documenti in formato digitale.

Non riguarda solo la pubblica amministrazione, in quanto parte delle norme in esso contenute si applicano anche ai privati.

Le norme più significative che contiene sono disposizioni sul documento informatico, la firma elettronica e la firma digitale.

IL CODICE DELL‘ AMMINISTRAZIONE DIGITALE
D.LGS. 7 marzo 2005 n.82

L'Italia è stato il primo paese dell’Unione Europea che, nel 1997, si è dotato di una legge sugli argomenti dei documenti in digitale: la Bassanini 1, che aveva come scopo quello di semplificare la comunicazione tra pubbliche amministrazioni e tra pubblica amministrazione e cittadini.

IL CODICE DELL' AMMINISTRAZIONE DIGITALE
i diritti digitali di cittadini ed imprese

Una volta realizzato un sistema che conferisse alla comunicazione digitale le stesse garanzie di certezza ed affidabilità di quello tradizionale, il Codice dell'Amministrazione Digitale ha assegnato ai privati un vero e proprio diritto di usarlo nei rapporti con le Pubbliche Amministrazioni. Sotto questo profilo, il CAD delinea e definisce in modo compiuto il valore legale della trasmissione telematica dei documenti informatici e le condizioni di validità per l'invio digitale di istanze e dichiarazioni.

IL DOCUMENTO INFORMATICO

Il Codice dell'Amministrazione Digitale (CAD-D.Lgs 82/2005) definisce il **documento informatico** come **"rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti",** in contrapposizione al **documento analogico, "rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti"** e lo inquadra come elemento centrale di quel processo di innovazione della Pubblica amministrazione finalizzato alla completa digitalizzazione delle pratiche amministrative.

IL DOCUMENTO INFORMATICO

Art. 23-ter. Documenti amministrativi informatici.

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono **informazione primaria ed originale** da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

l'informazione digitale ha lo stesso valore dell'informazione prodotta su supporto cartaceo

IL DOCUMENTO INFORMATICO

Art. 40. Formazione di documenti informatici.

1. Le pubbliche amministrazioni **formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici** secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.

IL DOCUMENTO INFORMATICO

Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni.

1. Le pubbliche amministrazioni **valutano in termini di rapporto tra costi e benefici il recupero** su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71. rt. 23-ter.

FORMA DEI DOCUMENTI INFORMATICI

Il nostro Codice Civile conserva il principio della libertà della forma e permette la conclusione di contratti anche in forma orale o tacita.

Secondo il nostro ordinamento giuridico vi sono tre diverse forme:

- ***forma per la validità del contratto*** **(ad substantiam)** la forma per l'esistenza del contratto stesso. Alcuni contratti, come ad esempio i contratti per l'acquisto di beni immobili, di costituzione di società, di donazione, richiedono questa forma per essere contratti validi, pena la nullità del contratto stesso ai sensi dell'Art. 1350 del Codice Civile. La donazione è un caso significativo del significato della forma per la validità: la donazione è una volontà rara, e il legislatore vuole la certezza che la volontà sia reale. La forma per la validità si può avere con il documento informatico sul quale sia stata apposta firma digitale o firma elettronica qualificata, secondo l'Art. 20 comma 2, che è il solo a poter essere equivalente a scrittura privata, scrittura privata autenticata, o atto pubblico (dipendentemente da come viene redatto e firmato).

FORMA DEI DOCUMENTI INFORMATICI

- ***forma per la prova*** **(ad probatione)** forma per provare il contratto in giudizio. Ad esempio per i contratti di assicurazione non è richiesta la forma scritta perché il contratto sia valido, ma solo per dimostrare di averlo concluso.

- ***forma scritta a fini informativi*** talvolta è richiesta la comunicazione di alcune informazioni per iscritto. Si tratta di una forma particolare, per la quale non servono firme o notai, la sola richiesta è che le in informazioni vengano veicolate in forma scritta, stampata, in un formato durevole, principalmente allo scopo di poter essere rilette a distanza di tempo. Il documento informatico è idoneo a costituire forma scritta per fini informativi, secondo l'Art. 20 comma 1bis, in modo valutato dal giudice caso per caso.

Art. 20. Documento informatico

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

Art. 20. Documento informatico

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

Art. 21. Valore probatorio del documento informatico sottoscritto

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.
3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Art. 25. Firma autenticata

L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

Art. 25. Firma autenticata

La procedura per apporre una firma autenticata ha un funzionamento analogo alla scrittura privata autenticata: ci si presenta dal notaio(o dal pubblico ufficiale) con un documento di identità e il certificato della firma, e si appone la firma in sua presenza. Il notaio aggiunge al documento una parte in cui attesta che la firma è stata apposta in sua presenza e che lui ha verificato l'identità del firmatario e il suo certificato, e firma questa dichiarazione con la propria firma digitale. In più, il notaio afferma, accerta, anche che l'atto non sia contrario all'ordinamento giuridico, cosa che non è tenuto a fare nel caso della scrittura privata autenticata.

La firma autenticata esclude l'utilizzo del dispositivo di firma da parte di un altro, e di conseguenza esclude la possibilità di disconoscimento della firma. Ne deriva un'efficacia probatoria maggiore rispetto alla scrittura privata autenticata: la firma è già legalmente riconosciuta.

TRASMISSIONE INFORMATICA DEI DOCUMENTI
Art. 45. Valore giuridico della trasmissione

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Art. 47
(Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Art. 47
(Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di protocollo informatizzato;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005.

Art. 47
(Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

3. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a:

a) istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, per ciascun registro di protocollo;

b) utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Art. 48 (Posta elettronica certificata)

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005.

2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, ed alle relative regole tecniche.

Art. 48 (Posta elettronica certificata)

La posta elettronica certificata nasce per le comunicazioni tra/con le pubbliche amministrazioni (ma può essere utilizzata anche in rapporti tra privati) e fornisce le stesse garanzie della raccomandata con ricevuta di ritorno, ovvero che il documento in questione sia stato effettivamente ricevuto dal destinatario. Questo è garantito dai provider stessi, che certificano l'avvenuto invio e l'avvenuta ricezione.

Possedere una casella di posta elettronica certificata (PEC) era inizialmente una scelta libera, basata sul consenso. Ora non è più così, e la PEC è obbligatoria, oltre che per le pubbliche amministrazioni, per le società di nuova costituzione e per i professionisti iscritti in un albo (a partire da fine novembre 2009)

FIRME E CERTIFICATI

Firma Elettronica

Il CAD definisce la **firma elettronica** come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione e identificazione informatica. Il fine della firma elettronica è consentire di identificare elettronicamente una persona. Esempi di firma elettronica possono essere password, badge, smartcard, o controllo delle impronte digitali.

Il **livello di sicurezza** di questi sistemi è molto variabile, si pensi a confrontare un pin a 5 cifre come quello del bancomat con una scansione della retina, eppure rientrano nella stessa classificazione dal punto di vista giuridico. Vedremo come la firma elettronica nel nostro ordinamento giuridico non dia grandi garanzie, proprio perché il livello di sicurezza che permette non è fisso, ed anzi la sua valutazione è soggetta alla discrezionalità del giudice.

FIRME E CERTIFICATI

Firma Elettronica Avanzata (FEA)

Il CAD la definisce come:

insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

FIRME E CERTIFICATI

Firma Elettronica Avanzata (FEA)

In sostanza la FEA è una firma riferita ad un documento specifico che permette dal documento di identificare in maniera certa il firmatario e di rilevare anche se il documento stesso è stato modificato dopo la firma. Il firmatario, ovviamente, deve avere il controllo esclusivo sui mezzi per apporre questo tipo di firma. Un esempio di tale firma è il processo di firma grafometrica che soddisfa i requisiti prescritti dalle regole tecniche di cui al **D.P.C.M. 22 febbraio 2013**. Per esempio, è la firma apposta su un tablet negli uffici postali o in banca. Un principio generale di queste tipologie di **firma grafometrica** è che esse collezionano dati biometrici del firmatario (es. pressione, velocità di firma, tratto ecc.) e li "fondono" in maniera permanente al documento da firmare in maniera tale che questi dati biometrici non siano più intellegibili a chi accede al documento.

FIRME E CERTIFICATI

Firma Elettronica Avanzata (FEA)

La legge riconosce alla firma elettronica avanzata un ambito di applicabilità inferiore a quello della firma digitale, in quanto la firma elettronica avanzata non può essere usata per i contratti che trattano vendite o locazioni di immobili e hanno valenza solo nei rapporti tra firmatario e controparte che gli ha proposto di usare quella particolare soluzione di firma, non ha cioè una valenza verso tutti come la firma digitale. Questo motivo la rende non adatta per i documenti di una pubblica amministrazione e, dunque, il CAD limita la sua usabilità solo ai documenti interni ad un procedimento amministrativo.

FIRME E CERTIFICATI

Firma Elettronica Avanzata (FEA)

il trattamento dei dati biometrici presuppone:

il rispetto del D.Lgs. 196/2003 e del **Provvedimento Garante per la Privacy n. 513 del 12 novembre 2014**

il consenso al trattamento del firmatario il quale “fornisce” i suoi dati esclusivamente per le finalità di firma del documento in questione

FIRME E CERTIFICATI

Firma Digitale

Ai fini del presente codice si intende per **firma digitale** un particolare tipo di firma elettronica avanzata 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.

Concretamente, si tratta della tecnologia crittografica a chiave asimmetrica, detta anche a chiave pubblica. Una chiave è, in termini semplici, un codice.

La firma digitale corrisponde quindi a tutti gli effetti alla firma autografa.

Poter identificare la provenienza di un documento significa poter fare un'attribuzione, con la firma si attribuiscono le dichiarazioni del documento al titolare della firma, se ne attesta la provenienza. Essendo la procedura di apporre una firma digitale un'elaborazione sull'intero documento, essa garantisce anche l'integrità del documento stesso.

FIRME E CERTIFICATI

Firma Elettronica Qualificata

Ai fini del presente codice si intende per **firma elettronica qualificata** la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica.

FIRME E CERTIFICATI

Certificato Elettronico

Ai fini del presente codice si intende per **certificati elettronici** gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità informatica dei titolari stessi. I certificati elettronici di certificazione sono rilasciati da una cosiddetta autorità di certificazione (accreditata/certificata) la quale ha l'onere di accertare l'identità della persona fisica. Non solo, la responsabilità dei certificatori è molto più elevata: devono gestire anche la revoca e la sospensione dei certificati in modo sicuro e corretto.

Cenni sulla conservazione valida sotto il profilo giuridico del documento informatico

Art. 44 (Requisiti per la conservazione dei documenti informatici)

1. Il sistema di conservazione dei documenti informatici garantisce:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

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, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

Copie e duplicati di un documento informatico

Il documento informatico deve essere formato e firmato digitalmente nel rispetto delle regole tecniche di cui al DPCM 13 novembre 2014

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

redazione con software;

acquisizione per via telematica o su supporto informatico;

acquisizione della copia per immagine su supporto informatico di un documento analogico;

Copie e duplicati di un documento informatico

acquisizione della copia informatica di un documento analogico;

registrazione informatica delle informazioni risultanti da transazioni o processi informatici;

presentazione telematica di dati (moduli o formulari resi disponibili all'utente);

generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Copie e duplicati di un documento informatico

Il documento informatico assume la caratteristica di **immodificabilità** se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione

Le caratteristiche di **immodificabilità e di integrità** sono determinate da una o più delle seguenti operazioni:

la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
l'apposizione di una validazione temporale;
il trasferimento con PEC con ricevute complete;
la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
il versamento ad un sistema di conservazione.

Copie e duplicati di un documento informatico

La **staticità** di un documento informatico si realizza attraverso l'uso di un formato c.d. "statico" che, cioè, non contenga campi che consentano delle modifiche di alcune parti del documento stesso non rilevabili alla verifica della firma. Sono formati statici il PDF/A, l'XML, EML, i formati immagine (ad es. TIFF), i formati testo come il TXT.

Come effettuare una copia informatica di un documento analogico

Il duplicato informatico di un documento informatico è ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario:

copia/incolla del file-documento.

Come effettuare una copia informatica di un documento analogico

Il duplicato informatico di un documento informatico è ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario:

copia/incolla del file-documento.

Il documento di risulta è identico a quello originale, a sua volta è un documento unico che pertanto non necessità di attestazioni di conformità.

Come effettuare una copia informatica di un documento analogico

Se il documento non firmato viene prelevato dai siti delle altre scuole o di altre PA, non potendo assumere a protocollo e conservare documenti privi di firma digitale, è necessario che il Dirigente scolastico ne attesti la conformità all'originale "visto" sul sito web interessato fornendo tra le altre informazioni anche i dati relativi all'URL di provenienza, alla data ed all'ora di prelevamento. l'attivazione di una procedura (anomala) di accoglimento con firma digitale del Dirigente scolastico che responsabilmente riconosce nel mittente identità certa in quanto il documento è dotato di firma elettronica

PIANO NAZIONALE SCUOLA DIGITALE
PNSD

E’ il documento di indirizzo del MIUR pensato per guidare le scuole in un percorso di **innovazione e digitalizzazione**, come previsto nella riforma della Scuola approvata dalla Legge 107/2015 – La Buona Scuola.

Punta a introdurre nuove **tecnologie** nelle scuole, a diffondere l’idea di **apprendimento** permanente (**lifelong learning**) ed estendere il concetto di scuola dal luogo fisico a spazi di apprendimento virtuali.

La normativa di riferimento del PNSD:

- Legge 107 del 13 luglio 2015 articolo 1 commi 56-57-58-59
- DM 851 del 27 ottobre 2015 «Piano Nazionale per la scuola Digitale»

L’INNOVAZIONE TECNOLOGICA NELLE SCUOLE

NELLE SCUOLE L’INNOVAZIONE TECNOLOGICA VIAGGIA ANCHE ATTRAVERSO IL PORTALE MIUR CHE CONSENTE L’ACCESSO ALL’AREA RISERVATA SIDI.

ATTRAVERSO IL SIDI E’ POSSIBILE ACCEDERE AD UNA MOLTEPLICITA’ DI FUNZIONI CHE HANNO CONSENTITO LA DEMATERIALIZZAZIONE E LA DIGITALIZZAZIONE DI MOLTI PROCEDIMENTI AMMINISTRATIVI.

DIVERSE SONO LE PIATTAFORME DIGITALI A TALE SCOPO PENSATE.

NAVIGHIAMO SU ALCUNE DI QUESTE PER VEDERNE LE FUNZIONALITA’.

LE PIATTAFORME DIGITALI MI

https://www.istruzione.it/accesso-sidi/

https://www.istruzione.it/pon/

https://sofia.istruzione.it/

https://www.miur.gov.it/innovazione-digitale

https://www.miur.gov.it/la-piattaforma-e-learning

Se di tanto in tanto
non hai degli insuccessi,
è segno che non stai facendo nulla di
davvero innovativo

Woody Allen