STUDIO LEGALE LISI

La forma scritta informatica tra firma digitale e firma biometrica e i processi di conservazione a norma

A cura di Andrea Lisi

Avvocato specializzato in diritto dell' ICT e privacy

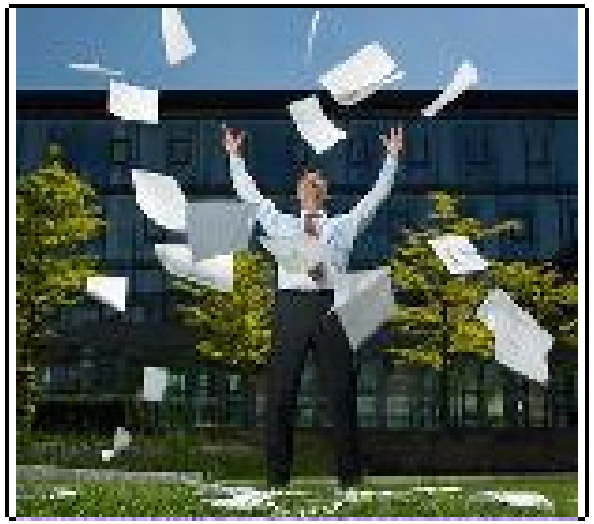
Presidente dell'associazione ANORC

Con il patrocinio di

Digital & Law
Department
www.studiolegalelisi.it

ANORC

Cosa sta succedendo in Italia?

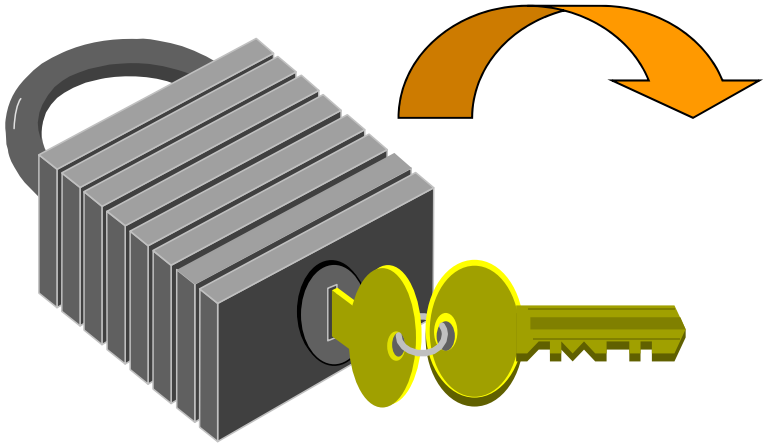


Verba volant, scripta manent?

Caio Titus nella Società Digitale

Ecco cosa ci circonda: una P.A. ormai Digitale

La rivoluzione disegnata nel Codice dell'Amministrazione Digitale



DIPENDENTI:
- e-mail, pec e firma digitale
-protocollazione informatica
-archiviazione e gestione documentale
-privacy e sicurezza informatica

DECERTIFICAZIONE

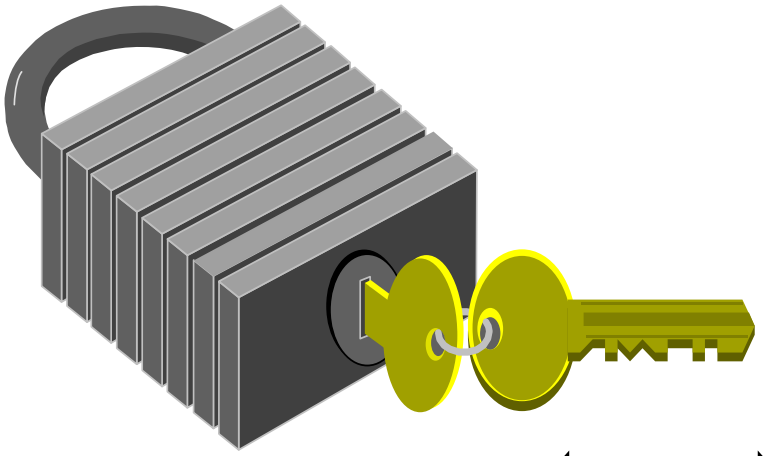
Altre Pubbliche Amministrazioni o imprese

Destinatari del servizio:
- pubblicità legale on line
- trasparenza e accessibilità
- formulari on line
- Sportelli e procedimenti on line

Connettività
E-government
E-procurement
Reti di P.A.

E-GOV

La multicanalità della PA digitale



INFORMAZIONI GENERALI:
- e-mail semplice
- portali informativi ad accesso libero
- chioschi telematici
- tv digitale
- sms
- call center

Formulari on line
- area riservata previa registrazione

Istanze on line e dichiarazioni:
- PEC e autenticazione informatica
- firma digitale (e FEA)
- telefax

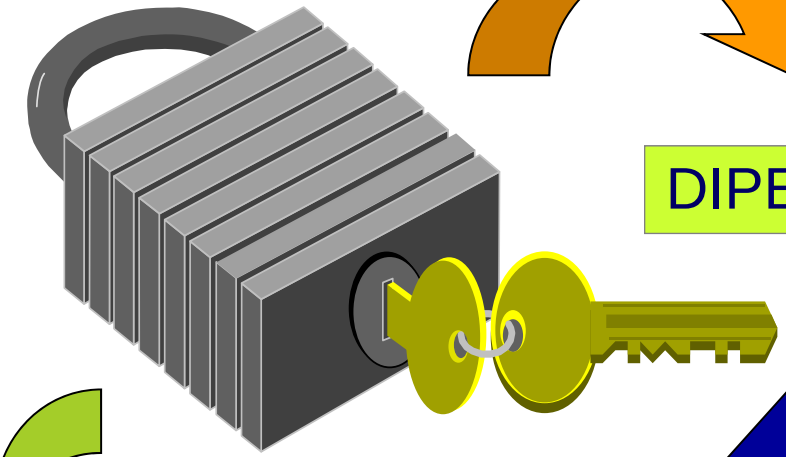
ATTENZIONE:
SICUREZZA INFORMATICA

Attivaz. procedimenti e transazioni
- autenticazione informatica
- posta certificata + firma digitale
- pagamenti elettronici

Comunicazioni Digitali e Imprese:

la chiave del successo nella Società dell'Informazione

P.A.D.



DIPENDENTI (INTRANET)

Fornitori/imprenditori
(extranet - B2B)

CLIENTI/UTENTI (B2C)

servizi on line di comunicazione
(email, sms, mms, siti web, blog, social etc.)

Distretti industriali
Filiere
Consorzi
Gruppi di imprese

E-marketplaces

Le norme ci sono?

PRINCIPALI FONTI NORMATIVE IN MATERIA DI DIGITALIZZAZIONE DOCUMENTALE

Documento Informatico, Firma digitale e Conservazione sostitutiva:

- **Codice della Pubblica Amministrazione Digitale (D. Lgs. 82/2005)**
- **Codice della Privacy (Allegato B del D. Lgs. 196/2003)**
- **Deliberazione CNIPA del 19 febbraio 2004 n. 11 (regole conservazione)**
- **DPCM del 30 marzo 2009 (Regole tecniche firma digitale)**
- **Deliberazione CNIPA del 21 maggio 2009 n. 45 (specifiche tecniche)**
- **DPR 11 febbraio 2005 n. 68 (Posta Elettronica Certificata)**

Fatturazione Elettronica e Conservazione Documenti Fiscali:

- **DMEF 23 gennaio 2004 (conservazione digitale documenti fiscali)**
- **D. Lgs. 20 febbraio 2004 n. 52 (fattura elettronica)**
- **Circolare Agenzia delle Entrate n. 45/E (del 19/10/2005)**
- **Circolare Agenzia delle Entrate n. 36/E (del 06/12/2006)**

Finanziaria 2005: comma 197 – e-cedolino

Finanziaria 2006: comma 51 – dematerializzazione corrispondenza

Finanziaria 2007 : trasparenza retribuzioni

Finanziaria 2008: commi 209-214 – obbligo di fatturazione elettronica alla PA – **New Decreto "Salva Italia"** (DL 201/2011 - conv in l. 214/2011)

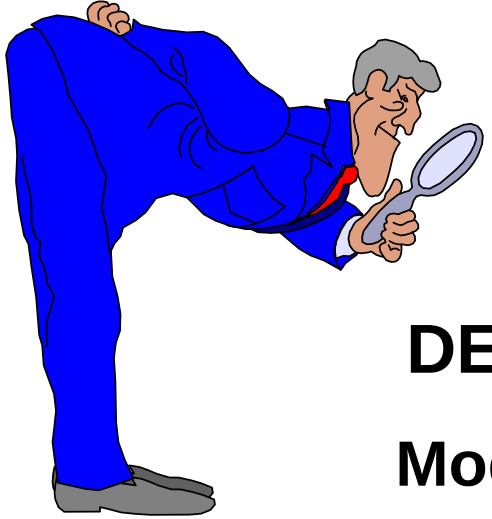
commi 589-593 – obbligo di PEC e telefonia VOIP

Manovra Fine Estate (DL 112/2008): artt. 39-40 – digitalizzazione LUL

Legge 18 giugno 2009 n. 69 – "taglia carta, revisione CAD, Voip, AOL"

DL anticrisi 78/2009 – convertito in Legge 3 agosto 2009, n. 102

- **D.L. 185/08 (L. 28 gennaio 2009 n. 2) – PEC obbligatoria per tutti e Documenti originali unici "smaterializzabili" senza notaio!**



Le ultime novità

DECRETO LEGISLATIVO 30 dicembre 2010, n. 235

Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

Nuove Regole Tecniche

decertificazione: art. 15 L. 183/2011 + Direttiva Pres. Consiglio Ministri 14/2011
decreto semplificazioni: DL 9 febbraio 2012 n. 5 convertito in Legge 4 aprile 2012 n. 35 (Agenda Digitale)
misure urgenti crescita Paese: DL 22 giugno 2012 n. 83 convertito in Legge 7 agosto 2012 n. 134 (Agenzia per l'Italia Digitale)

le <u>ultimissime novità sono davvero innovative?</u>

- **LEGGE 12 novembre 2011, n. 183** - *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato* (**Legge di stabilità 2012).**

- Decreto-Legge 9 febbraio 2012, n. 5, *Disposizioni urgenti in materia di semplificazione e di sviluppo* – Convertito, con modificazioni, dalla **LEGGE 4 aprile 2012, n. 35.**

- Decreto-Legge 7 maggio 2012, n. 52, *Disposizioni urgenti per la razionalizzazione della spesa pubblica* – Convertito, con modificazioni, dalla **LEGGE 6 luglio 2012, n. 94.**

- Decreto-Legge 22 giugno 2012, n. 83, *Misure urgenti per la crescita del Paese* - Convertito, con modificazioni, dalla **LEGGE 7 agosto 2012, n. 134.**

- Decreto-Legge 6 luglio 2012, n. 95, *Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini* - Convertito, con modificazioni, dalla **LEGGE 7 agosto 2012, n. 135.**

Decreto crescita 2.0

Il documento informatico

di cosa stiamo parlando?

…del passaggio culturale, sociologico, economico e, quindi, giuridico da un documento pesante e statico ad un documento dinamico, che si condivide e che diventa “partecipativo”…

Il documento informatico è valido e rilevante, ma non è “carta informatica”:

Il documento informatico, quindi, non sempre è “forma scritta”

«**documento digitale**»: testi, immagini, dati strutturati, disegni, programmi, filmati formati tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica, di cui sia identificabile l'origine
(art. 1 lett. d) DMEF 23 gennaio 2004 - Modalita' di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di suppporto)
“**documento informatico**: rappresentazione informatica di atti, fatti, **dati** giuridicamente rilevanti” (C.A.D., art. 1, comma 1°, lett.p)
documento informatico penalmente rilevante
art. 491 bis – (…) per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli (L. 48/2008).

Un esempio di Documento Informatico con firma digitale: Siamo sicuri di saperlo verificare?

un file p7m valido e rilevante

Definizione di formazione di documento informatico

Bozza Regole tecniche del documento informatico e gestione documentale

Versione del 05/08/2011

Art. 3 comma 1

La formazione del documento informatico comprende le attività di cui alle seguenti principali tipologie:

a) redazione tramite l'utilizzo di appositi strumenti software;

b) acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico, acquisizione per via telematica o su supporto informatico;

c) registrazione informatica delle informazioni risultanti da transazioni informatiche o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

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

Integrità e immodificabilità?

Ma quante firme ci sono?

Lo scopo della Normativa

***Garantire al Documento Informatico Amministrativo, Contabile e Fiscale*:**

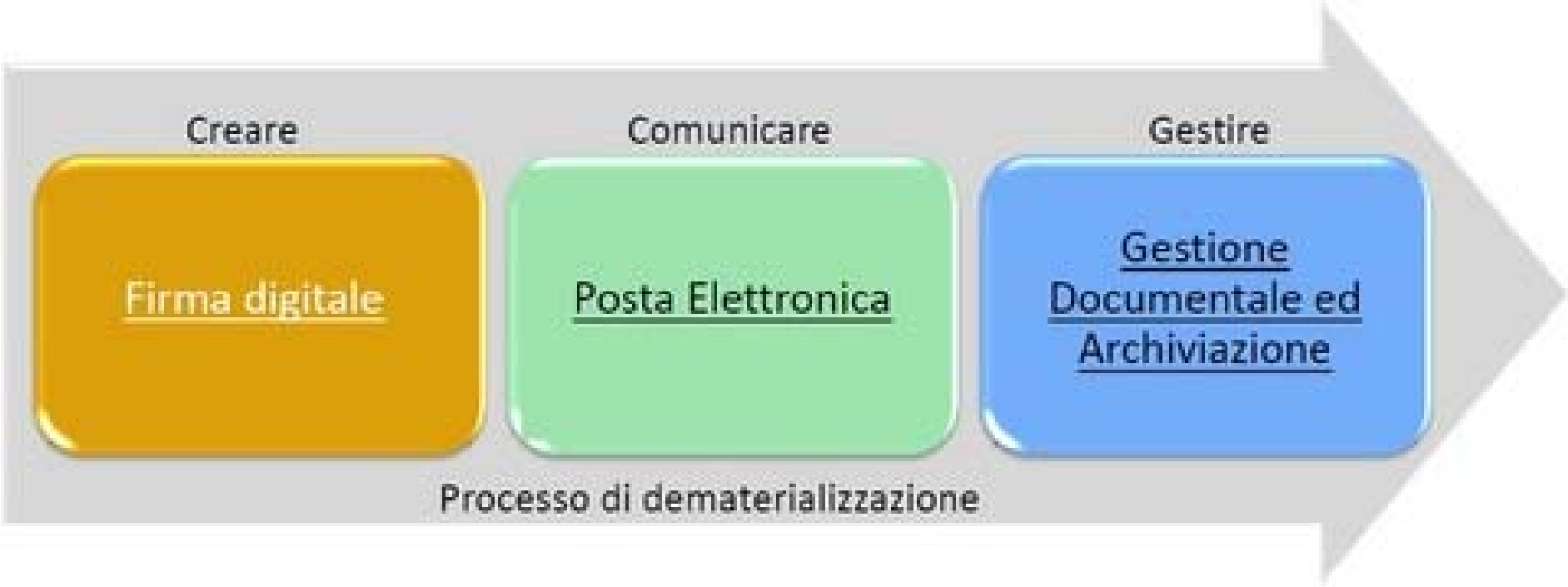
- **La paternità (Firma Digitale *o altri sistemi di identificazione*)**
- **L'integrità (Firma Digitale)**
- **La trasmissibilità informatica (PEC o SPC o EDI)**
- **la corretta gestione (archiviazione elettronica)**
- **La "memorizzazione digitale" nel tempo (Firma Digitale, Marca Temporale e Procedure di Sicurezza)**

attraverso una complessa procedura di conservazione

Massima attenzione ai formati documentali

N.B.: *Duplice funzione della firma digitale*

Processi corretti di digitalizzazione documentale



La legge attualmente in vigore e le sue definizioni

Il Codice della amministrazione digitale (art. 1)

Firma elettronica (lett. q) - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

Firma elettronica avanzata (lett. q-bis) - 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

Firma elettronica qualificata (lett. r) - 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

Firma digitale (lett. s) - Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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

→ *L'imputabilità giuridica*

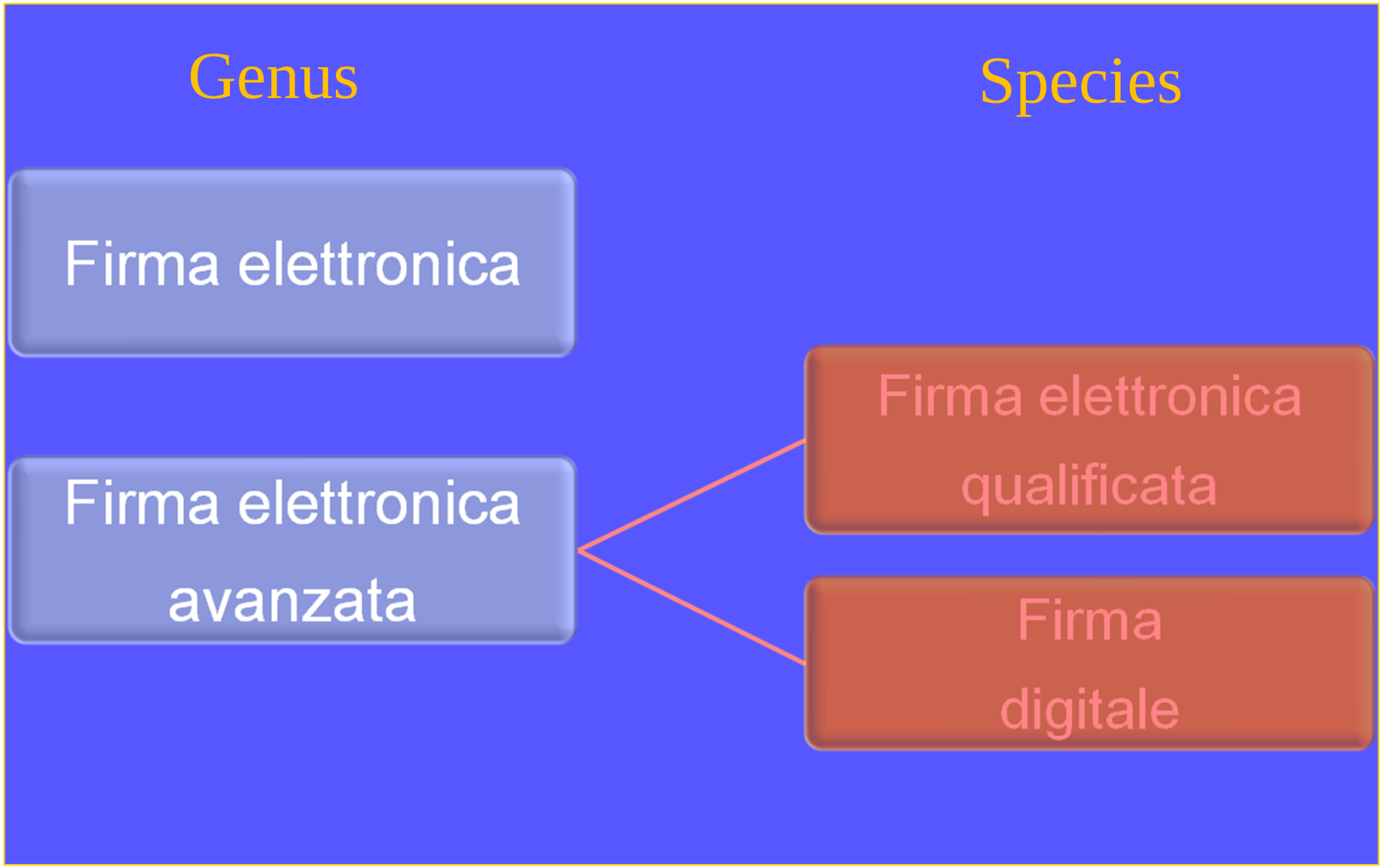
Invio istanze nelle PA:

-DPCM 6 maggio 2009: la PEC è sottoscrizione??

- art. 65 del CAD – invio delle istanze via PEC o con identificazione sul sito tramite CNS e CIE

→ *…forma scritta e firma anche a prescindere dalla firma digitale!*

Genus e species di firma elettronica in Italia



La legge attualmente in vigore e le sue definizioni

Il Codice della amministrazione digitale (artt. 20, 21)

1-bis. L'idoneità del documento informatico a soddisfare il requisito della **forma scritta** e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

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 elettronica avanzata**, **qualificata** o **digitale**, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, 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.

2-bis). Salvo quanto previsto dall'articolo 25, le **scritture private di cui all'articolo 1350**, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

→ *I formati documentali*

Le applicazioni nella **PA**:

-I procedimenti interni (art. 23 ter comma 2 e art. 34 comma 2)

- le regole tecniche per la firma elettronica avanzata

- le regole tecniche per la conservazione

→ *… la firma che non firma …*

FIRMA DIGITALE

valore formale e probatorio predefinito per legge

difficilmente disconoscibile

equivale alla sottoscrizione cartacea

associata alla marca temporale conferisce al documento certezza giuridica

FIRMA ELETTRONICA

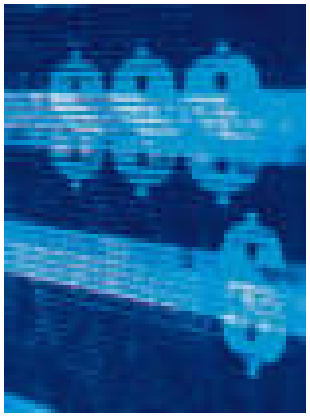
è genus indefinito

La sua valenza formale e probatoria è relativa

può essere facilmente disconoscibile

garantisce la paternità, non sempre l'autenticità

E la firma elettronica avanzata?



La firma elettronica avanzata

Le nuove regole Tecniche

La Firma Elettronica Avanzata, non è un determinato software, né una determinata tecnologia, ma è un sistema neutro, sicuro e affidabile che garantisca l'appartenenza di un documento informatico reso immodificabile ad un soggetto

Art. 56 Caratteristiche delle soluzioni di firma elettronica avanzata

1. Le soluzioni di firma elettronica avanzata devono 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, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
d) la possibilità di verificare che l'oggetto della sottoscrizione 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 di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati.

La sua valenza formale e probatoria dipende dal sistema che si sviluppa

E ricordiamoci sempre:
Articolo 1352 c.c. Se le parti hanno convenuto per iscritto di adottare una determinata forma per la futura conclusione di un contratto, si presume che la forma sia stata voluta per la validità di questo

***Esempio di firma elettronica avanzata**: strong authentication + sistema sicuro di transazione + sistema di conservazione dei log*

Art. 57 - Obblighi per i soggetti che erogano per proprio conto soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a) devono:

a) **identificare in modo certo l'utente**, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una **dichiarazione di accettazione delle condizioni del servizio da parte dell'utente**;

b) conservare per almeno venti anni la dichiarazione di cui al punto a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;

c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;

d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;

e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1, specificando le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto, pubblicandole anche sul proprio sito internet;

f) consentire l'uso della firma elettronica qualificata e della firma digitale, ove applicabile, in alternativa alla firma elettronica avanzata per i procedimenti per i quali è previsto l'uso della firma elettronica avanzata;

g) assicurare la disponibilità di un servizio di revoca relativo alla firma elettronica avanzata, ove applicabile, e un servizio di assistenza.

+ copertura danni sino a € 500.000 (copertura assicurativa) e pubblicazione su sito web del sistema di copertura

***Limiti d'uso**: La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a) (art. 60 Regole Tecniche)*

Non è prevista alcuna autorizzazione preventiva

Le domande:
-so quello che firmo?
-come associo la firma al documento?
-cosa conservo? e chi conserva?
-rilascio ricevute certe su ciò che si è firmato?
Etc.

La nuova moda della Firma «Grafometrica»

La firma sul Tablet

Le domande:
-so quello che firmo?
-come associo la firma al documento?
-cosa conservo? e chi conserva?
-rilascio ricevute certe su ciò che si è firmato?
Etc.

La firma biometrica

La prima firma biometrica è la sottoscrizione cartacea!

Il termine "riconoscimento biometrico" fa riferimento all'identificazione o alla verifica automatica dell'identità attraverso strumenti di valutazione di caratteristiche fisiche o comportamentali (Linee Guida CNIPA 2004)

Acquisizione sul documento dell'immagine della sottoscrizione di un soggetto → *Se non è verificabile il comportamento di chi firma, non è biometria e non crea problemi tecnici e di privacy, ma ha scarso valore giuridico*

Acquisizione evoluta sul documento di vari dati comportamentali di chi firma → *È la versione elettronica della sottoscrizione cartacea. Può essere di volta in volta verificabile la sua autenticità e non c'è centralizzazione di dati biometrici*

(può richiedere la necessità di interpello ai sensi dell'art. 17 Codice privacy e la sua valenza probatoria può essere robusta)

Acquisizione biometrica come credenziale forte di autenticazione → *Può servire a garantire un accesso riservato di transazione, ma anche come modello di sottoscrizione digitale e, quindi, garantire un accesso in remoto al proprio certificato di firma custodito da un HSM*

(rende necessario richiedere un interpello ai sensi dell'art. 17 Codice privacy e può servire per "sbloccare" in remoto certificati di firma digitale)

ART. 24 (Firma digitale)

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. **L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente**.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71 , la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Ma i giudici dicono qualcosa?

E i giudici che dicono?
Un po' di Giurisprudenza sui «dati informatici»:

- **L'ordinanza del 30-04-2011 del Tribunale di Catanzaro ha stabilito che il consenso manifestato attraverso il tasto negoziale** virtuale (c.d. *point&Click*) **è idoneo a perfezionare la conclusione del contratto** (relativamente al principio delle libertà delle forme). Tuttavia, la pronuncia in oggetto ha **escluso** che la medesima modalità di manifestazione del consenso possa validamente integrare la specifica approvazione per iscritto da parte del consumatore delle **clausole vessatorie**, richiesta ai fini dell'efficacia delle condizioni generali del contratto dall'art. 1341 codice civile. Al riguardo, il Giudice ha precisato che **tali clausole devono**, invece, **essere sottoscritte con firma digitale**, poiché la semplice sottoscrizione via web in modalità *point and click* non sarebbe idonea ad integrare la forma scritta richiesta dalla legge. L'ordinanza in oggetto stimola diverse interessanti riflessioni relativamente all'applicazione delle norme del Codice Civile e del Codice dell'Amministrazione Digitale

La Giurisprudenza:

- La terza sezione della **Corte di Giustizia Europea** con la sentenza 5 luglio 2012 relativa alla **causa C-49/11** affronta la complessa materia della protezione dei consumatori nei contratti a distanza sostenendo che "*l'articolo 5, paragrafo 1, della direttiva 97/7/CE del Parlamento europeo e del Consiglio, del 20 maggio 1997, riguardante la protezione dei consumatori in materia di contratti a distanza, deve essere interpretato nel senso che non soddisfa i requisiti da esso imposti una prassi commerciale che consista nel rendere accessibili le informazioni richieste dalla norma precitata solamente attraverso un collegamento ipertestuale a un sito Internet dell'impresa interessata, dal momento che tali informazioni non sono né «fornite» da tale impresa né «ricevute» dal consumatore, come prescrive la suddetta disposizione, e che un sito Internet non può essere considerato un «supporto duraturo» ai sensi del medesimo articolo 5, paragrafo 1".*

La Giurisprudenza:

- il TAR Puglia - Bari, Sez. I, con la sentenza n. 1019 del 24 maggio 2012 dichiara l'obbligatorietà della sottoscrizione dell'offerta con firma digitale in caso di gare telematiche

- una recente sentenza del **TAR Milano (**T.A.R. Lombardia Milano Sez. IV, Sent., 11-07-2012, n. 1942) ha annullato un provvedimento di esclusione dalla procedura di gara indetta da LOMBARDIA INFORMATICA SPA. Lombardia Informatica S.p.A. aveva provveduto all'esclusione dalla gara per la fornitura di soluzioni infusionali la Baxter S.p.A., società ricorrente, in quanto all'atto della presentazione dell'offerta in via elettronica, avrebbe sottoscritto ed immesso nel sistema un documento vuoto, file di dimensioni pari a 0 kb nonchè privo dei contenuti richiesti, in luogo della dichiarazione di offerta economica. La procedura di gara pubblica era gestita in via informatica per il tramite di piattaforma "SinTel". E' stato accertato che il sistema SInTel utilizzato non garantiva il tracciamento di ogni operazione compiuta sulla piattaforma, e l'inalterabilità delle registrazioni (log) di sistema, quali rappresentazioni informatiche degli atti e delle operazioni compiute, valide e rilevanti ai sensi di legge.

SICUREZZA AZIENDALE, RISK MANAGEMENT E CORRETTA CONSERVAZIONE DEI DATI

Provv. Garante 27/11/2008 sugli amministratori di sistema

Occorrerà inevitabilmente dotarsi di strumenti e meccanismi che permettano di evitare non solo la perdita di dati e informazioni importanti per l'azienda, ma anche la loro modifica o la loro alterazione, strumenti di gestione di tali documenti e atti che permettano di mantenerne la **stabilizzazione temporale e l' integrità complessiva** e che **permettano di risalire pacificamente al titolare del documento**, rendendo facilmente individuabile il soggetto cui quel documento o quella semplice informazione sono ascrivibili. Tutto questo nel rispetto della privacy.

Es. esibizione di file di log di navigazione in un giudizio di lavoro…

La precarietà della prova digitale non correttamente conservata…

Acquisizione di file di log da parte della PG tramite mera consegna dei dati da parte dell'ISP – obbligo di verifica circa le modalità della conservazione degli stessi allo scopo di assicurare la genuinità e l'attendibilità nel tempo – necessità – sussiste (**Sentenza Tribunale Chieti n. 175/05**)

Quali documenti sono digitalizzabili?

DOCUMENTI RILEVANTI AI FINI TRIBUTARI SMATERIALIZZABILI AI SENSI DEL DM 23 GENNAIO 2004

- Fatture, bollette, lettere, telegrammi ricevuti
- Distinte meccanografiche e registri (corrispettivi e registri fatture emesse)
- Il libro giornale e il libro degli inventari
- Le scritture ausiliarie nelle quali devono essere registrati gli elementi patrimoniali e reddituali
- Le scritture ausiliarie di magazzino
- Il registro dei beni ammortizzabili
- Il bilancio d'esercizio, composto da stato patrimoniale, conto economico e nota integrativa
- I registri prescritti ai fini IVA, quali ad esempio il registro degli acquisti, il registro dei corrispettivi, il registro delle fatture emesse
- Dichiarazioni fiscali, modulistica relativa ai pagamenti (ad esempio i modelli F23 ed F24), alle fatture e documenti simili
- I libri sociali
- Il libro delle adunanze e delle deliberazioni delle assemblee
- Il libro delle adunanze e delle deliberazioni del collegio sindacale
- Il libro delle adunanze e delle deliberazioni del comitato esecutivo
- Il libro delle adunanze e delle deliberazioni delle assemblee degli obbligazionisti
- Le disposizioni contenute nel DMEF 23 gennaio 2004, infine, si applicano alla relazione sulla gestione (art.2428 c.c.) e alla relazione dei sindaci (art. 2429 c,c.) e dei revisori contabili , che per legge devono essere allegate al bilancio d'esercizio.

Oggi comunque tutti i documenti possono nascere informatici o comunque sono digitalizzabili ex lege

Altre tipologie documentali:

- ***Documenti amministrativi***
- ***Documenti privacy***
- ***Contratti e atti di trasferimento quote societarie (DL 112/2008)***
- ***Documenti sanitari e amministrativi***
- ***Nota spese dipendenti e schede carburante***
- ***Libro Unico del lavoro (DL 112/2008 conv. L. 133/2008 + Circ. Min. Lavoro n. 20/2008)***
- ***Registri assicurativi***
- ***la corrispondenza telematica, la PEC***

Documenti analogici?

Documenti informatici?

Il Sistema di Conservazione Digitale dei documenti

…ma come si fa?

Un rapido sguardo alle regole generali…
(Codice dell'amministrazione digitale e Regole tecniche in vigore)

ART. 43 CAD (Riproduzione e conservazione dei documenti)

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui e' prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformita' dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.

La conservazione digitale non è una scelta eventuale, ma un dovere!

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.

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

1. Il sistema di conservazione dei documenti informatici assicura:

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;

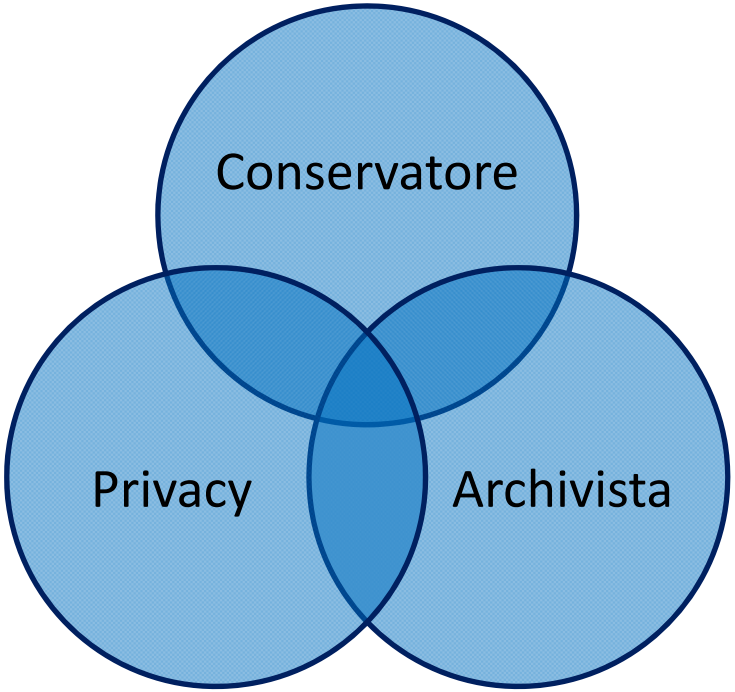
d) il rispetto delle **misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196**, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

Chiave interpretativa per la normativa sulla conservazione sostitutiva e sulla fatturazione elettronica

Art. 44, comma 1 bis CAD (Requisiti per la conservazione dei documenti informatici) - NEW

Il sistema di conservazione è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

La conservazione digitale si fa in tre!



51. CAD Sicurezza dei dati.

1. Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.
2. 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.

Non c’è conservazione senza sicurezza informatica

Nuovo CAD – delega contenuta nell'art. 33 L. 69/20098

Dopo l'articolo 50 del decreto legislativo 7 marzo 2005, n. 82, è inserito il seguente: "**Art. 50-bis** - (Continuità operativa). - 1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono :

a) **il piano di continuità operativa**, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) **il piano di disaster recovery**, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA assicura l'omogeneità delle soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.".

In vigore dall' aprile del 2012!

Sistema di gestione e conservazione informatica dei documenti e dei dati informatici rilevanti

Sviluppo di un sistema informatico

Analisi organizzativa

Change Management

Sicurezza informatica

privacy

Analisi dei processi di gestione dei flussi documentali
-Mappatura processi
- Rilevazione ruoli e responsabilità

Reingegnerizzazione di tutti i procedimenti
- Ridefinizioni ruoli e responsabilità
- Analisi costi/benefici

Formazione Comunicazione

Conservazione sostitutiva

D. Lgs 231/2001

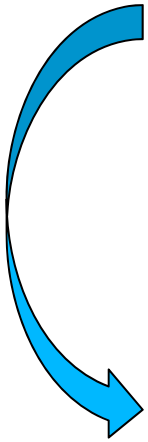
L'ORGANIZZAZIONE

In strutture complesse gerarchia di responsabili a più livelli

La Governance del patrimonio informativo di una società o una PA: Compliance normativa nella Società dell'Informazione

I problemi del documento informatico e dell’archiviazione sostitutiva…

- **necessità della formazione del personale**
- **riorganizzazione di tutti i processi**
- **necessità di nuovo hardware e software**
- **presenza di una normativa in costante evoluzione e ancora non completamente soddisfacente**



Possibilità di procedere parzialmente nel processo (inevitabile) di conservazione sostitutiva e di affidarsi a terzi, **esternalizzando alcuni servizi**

Riferimento temporale/marca temporale

Dematerializzazione e conservazione sostitutiva (C.A.D. e Del. CNIPA n. 11/2004)

Attribuibilità e immodificabilità del documento

Firme Elettroniche/ Digitali e Riferimenti Temporali su singoli documenti

Formazione del documento o sua "riproduzione sostitutiva"

Archiviazione Elettronica

Conservazione documento

Firma digitale + Marca Temporale sul lotto di documenti

Sicurezza della conservazione

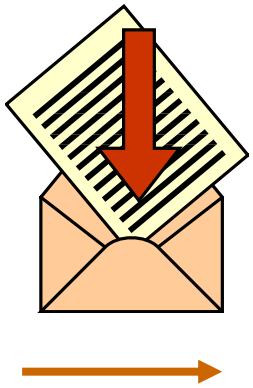
Misure di sicurezza: back up, disaster recovery e restore

Outsourcing (art. 5 Del. CNIPA)

ART. 12 5-bis CAD. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

i servizi in outsourcing

Cliente



Outsourcer

Fatturazione

Chi firma?

Chi controlla?

Chi è responsabile?

Servizi di conservazione con nomina quale responsabile esterno della conservazione sostitutiva

L'"esternalizzazione" di alcuni processi aziendali fortemente specializzati e complessi

Verifica e certificazione dei processi

Dal “nuovo” Codice della Amministrazione Digitale:

Art. 44, comma 1 ter (Requisiti per la conservazione dei documenti informatici) - NEW

Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall’articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad **altri soggetti**, **pubblici o privati**, che offrono **idonee garanzie organizzative e tecnologiche**.

Possibilità anche per la P.A. di affidare in outsourcing i processi di conservazione digitale e ottenere la “certificazione di conformità” dei relativi processi!

Grazie per l'attenzione

...e per contatti o ulteriori informazioni:

Avv. Andrea Lisi

Digital&Law Department Studio Legale Lisi

www.studiolegalelisi.it

Tel. 0832/256065 – Fax 0832/520140

Digital & Law
Department
www.studiolegalelisi.it