FACOLTÀ DI INGEGNERIA DI PARMA
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PARMA

CORSO PREPARATORIO AGLI ESAMI DI STATO DI ABILITAZIONE ALL'ESERCIZIO DELLA PROFESSIONE DI INGEGNERE

Sommario

Web link 2
Riferimenti istituzionali 2
Altri siti 2

Modalità di accesso e conservazione dei dati personali (privacy) 3
Privacy: DL 196 4
La sicurezza delle informazioni: Concetti generali 11
La documentazione 18
La sicurezza nella "normale attività di lavoro" 21
Preparazione dell'audit di certificazione 26

Firma elettronica, firma elettronica qualificata, firma digitale 29
A cosa servono 29
Firma elettronica 29
Firma elettronica qualificata 29
Firma digitale 29
Crittografia asimmetrica 29
Un esempio 29

Posta Elettronica Certificata (PEC) 31
Cosa viene certificato 31
Elementi di sicurezza 31
Posta elettronica e PEC 31
Ricevute e buste di trasporto 31
PostaCertificat@: l'offerta PEC dellaPubblica Amministrazione 32

Carta identità elettronica 33
Carta Nazionale dei Servizi (CNS) 34

La Carta sanitaria elettronica 35

Codice dell'Amministrazione Digitale (CAD) 37
Il decreto crescita 2.0 modifica il CAD 37
Le nuove disposizioni per la modulistica tipo 37
Il decreto spending review modifica il CAD 37
Il decreto semplificazioni modifica il CAD 38
Principi Guidaguida del nuovo CAD 38
Ora si può fare 39
I tempi di applicazione 41
Glossario del Codice dell'Amministrazione digitale 43

Diritto d'autore sul software 46
Principi generali 46
Ambito della tutela 46
Fondamento del diritto 46
Facoltà del titolare 46
Contenuto 47
Originalità dell'opera 47
Contraffazione 47
La tutela giuridica 49
Categorie di software 50

Principi relativi alle intrusioni nei sistemi informatici. 52
Rischi di una intrusione 52
Gli attacchi e le vulnerabilità 52
Tipologie di attacco 52
Internet 52
Wardialing 52
Web Application 53
Wireless 53
Provenienza dell'attacco 53
Attacco esterno 53
Attacco interno 54
Apparecchiature da verificare 54
Rilevazione dell'intrusione e ripristino dei sistemi 54
Modifica delle password sui sistemi 54
Reinstallazione completa dei sistemi compromessi 55
imozione dei programmi utilizzati e delle modifiche 55
Reinstallazione dei programmi eseguibili e dei file binari dai supporti di distribuzione originali. 55
Revisione delle configurazioni del sistema. 55
Eliminare vulnerabilità e correggerle. 55
Verifica dei requisiti e della tempistica per il ritorno alla normale operatività. 55
Azioni conclusive 56

Web link

Riferimenti istituzionali

www.italia.gov.it
www.digitpa.gov.it
www.postacertificata.gov.it
www.garanteprivacy.it

Altri siti

www.techweb.com/encyclopedia/

Modalità di accesso e conservazione dei dati personali (privacy)

Ovvero:

- Privacy: DL 196
- La sicurezza delle informazioni: Concetti generali
- Sistema Sicurezza: ISO 27001
- La documentazione
- La sicurezza nella “normale attività di lavoro”
- Preparazione dell’audit di certificazione

La Legge

In Italia la privacy è tutelata dal decreto legislativo n° 196 del 30 giugno 2003 in vigore dal primo gennaio del 2004 "Codice in materia di protezione dei dati personali".

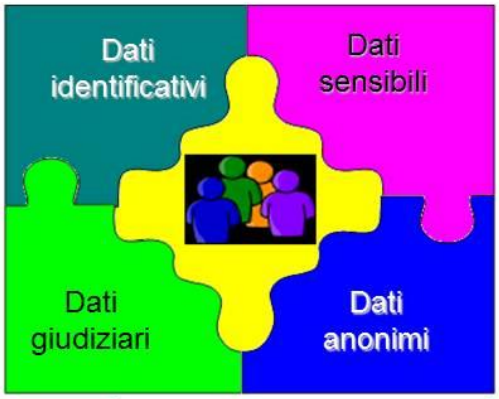
Sono le informazioni relative a persone fisiche o giuridiche che ne consentono l'identificazione direttamente o indirettamente. Il codice li definisce così:

Qualsiasi informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Classificazione dei dati personali

Dati Identificativi
Dati che permettono l'identificazione diretta Dell'interessato

Dati Giudiziari
Dati idonei a rivelare informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato



Dati Anonimi
Dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Dati Sensibili
dati che rivelano: l'origine razziale ed etnica; le convinzioni religiose, filosofiche o di altro genere; le opinioni politiche; l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale; lo stato di salute e la vita sessuale.

Trattamento

Per **trattamento** s'intende

"qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la

raccolta	**registrazione**
organizzazione	**conservazione**
elaborazione	**modificazione**
selezione	**estrazione**
raffronto	**utilizzo**
interconnessione	**blocco**
diffusione	**comunicazione**
cancellazione	**distruzione**

Trattamento : FIGURE

Il codice individua essenzialmente tre figure:

Titolare

Responsabile

Incaricato

Il loro compito è quello di garantire il trattamento corretto e la sicurezza dei dati

Titolare

Responsabile

Incaricato

Trattamento : FIGURE

Titolare

Persona fisica o persona giuridica a cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

AL TITOLARE COMPETONO TUTTI GLI ADEMPIMENTI FORMALI E SOSTANZIALI RICHIESTI DALLA NORMATIVA.

TRA QUESTI, IL TITOLARE, DEVE
DEFINIRE E CONTROLLARE IL RISPETTO
DELLE MODALITÀ OPERATIVE SULLA SICUREZZA,
NOMINARE GLI INCARICATI
(esclusivamente persone fisiche)
PUÒ EVENTUALMENTE NOMINIARE I RESPONSABILI
(anche persona giuridica).

Trattamento : FIGURE

Responsabile

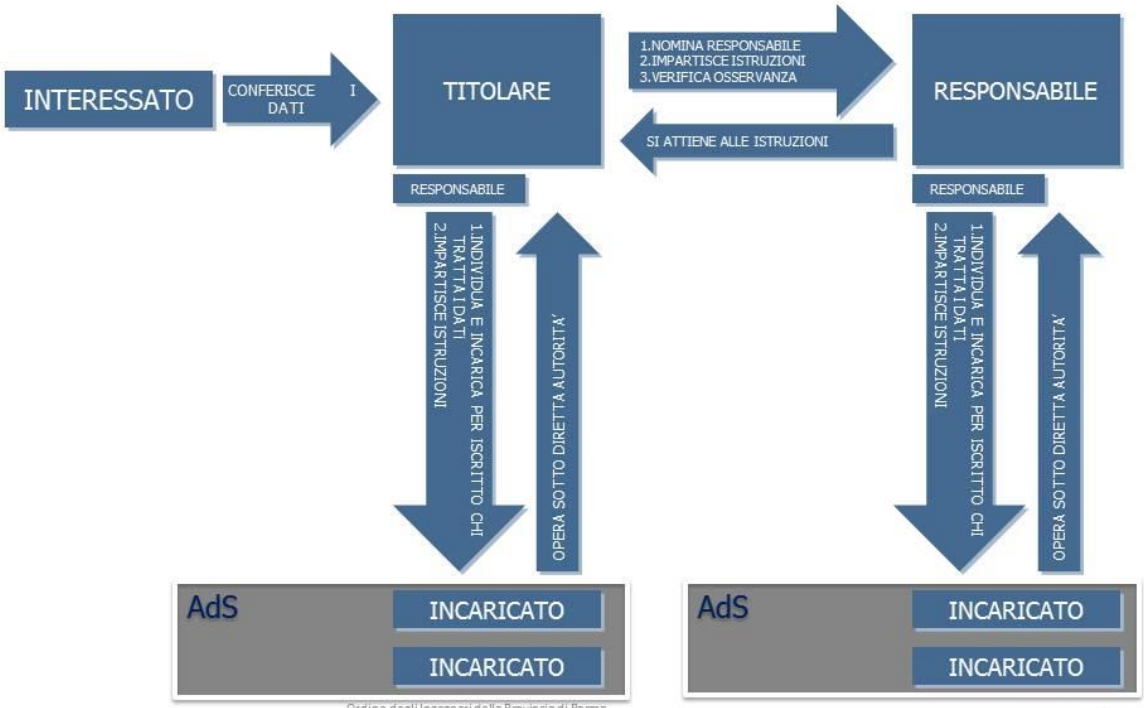
Persona fisica o persona giuridica preposti dal titolare al trattamento di dati personali

Incaricato

Ogni dipendente e' "**incaricato al trattamento**" con nomina formale, tramite lettera d'incarico, ai Rensponsabili delle Unità Operative che devono divulgare la designazione agli addetti dell'unità stessa.

Il trattamento dei dati personali richiede obbligatoriamente l'adozione di idonee e preventive misure di sicurezza, che chiunque essendovi tenuto omette di adottare è suscettibile di sanzioni penali e civili.

Trattamento



Trattamento : FIGURE

Amministratori di sistema

(Provvedimento del 27/11/2008)

"figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi"

In Azienda sono individuati di norma come Amministratori di Sistema gli addetti dell'Area tecnologica, dell'Ufficio Ispettorato e degli Uffici di Sviluppo Applicativo.

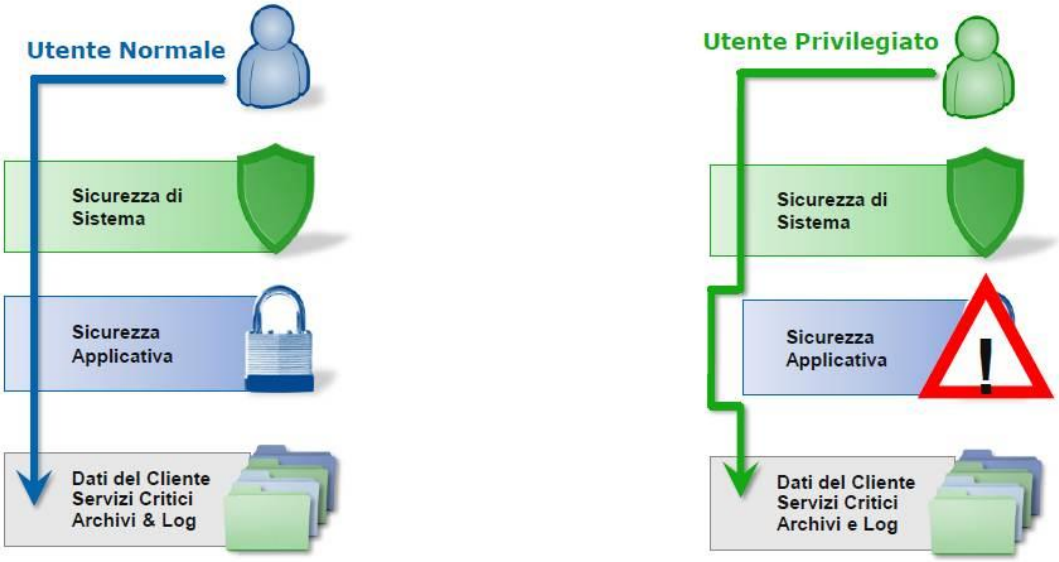
Perché individuare gli AdS

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

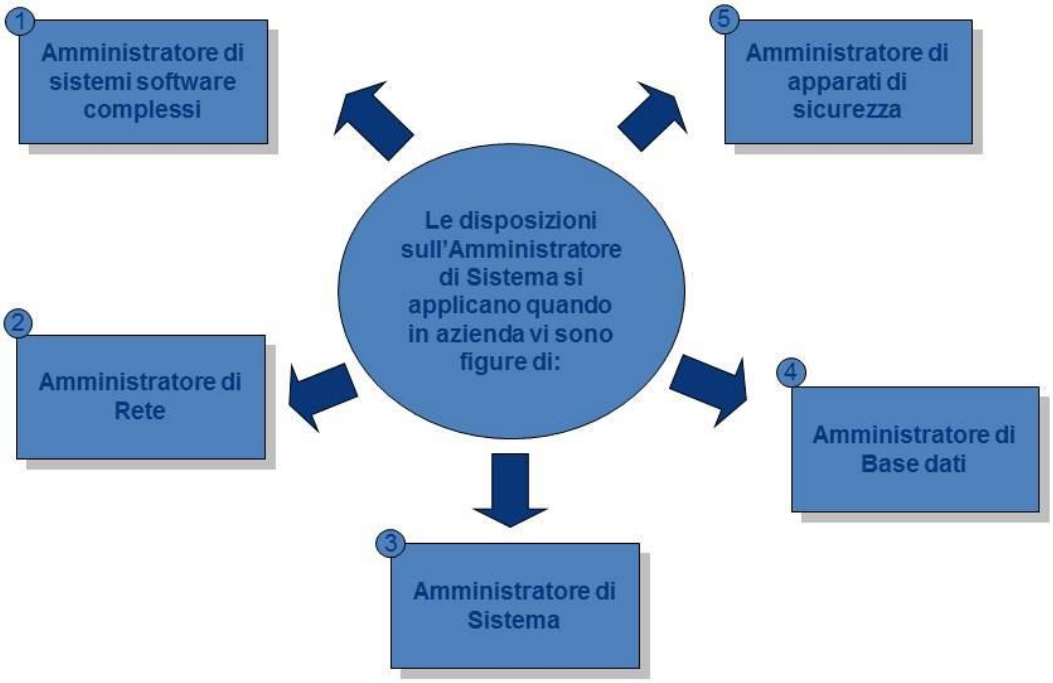
"Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo."

Comunicato stampa - 14 gennaio 2009

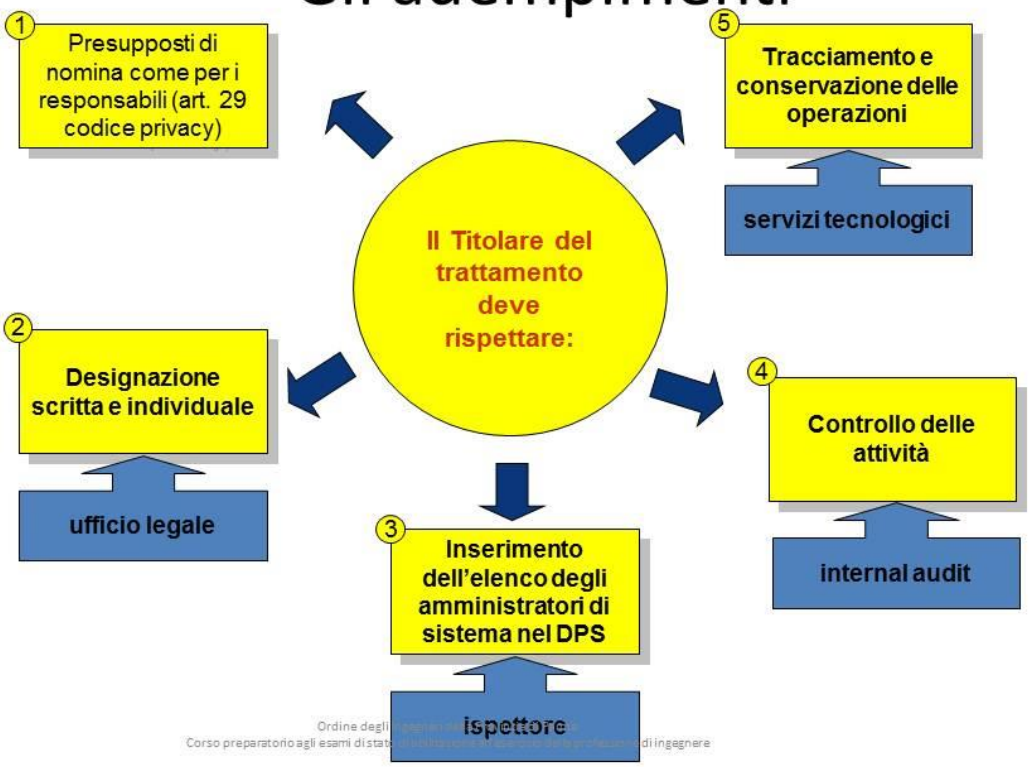
Come individuare gli AdS



Ambiti interessati



Gli adempimenti



Documento Programmatico sulla Sicurezza

- DPS: documento "ufficiale" che riporta le misure di sicurezza adottate o previste per garantire l'integrità, la disponibilità e la riservatezza dei dati.
- Funzione: illustra i trattamenti di dati effettuati dall'Azienda, i ruoli e le responsabilità, l'analisi dei rischi, le misure di sicurezza adottate e le relative verifiche in relazione ai dati oggetto del D.Lgs. 196/03 (Codice in materia di protezione dei dati personali)

Non più obbligatorio da decreto 5/12

Soppressione obbligatorietà documento programmatico

Con il decreto semplificazioni (D.L. n. 5/12) è stato soppresso a decorrere dalla scadenza del 31 marzo 2012 l'obbligo di redazione o aggiornamento:

- del Documento Programmatico sulla Sicurezza, compreso quello "semplificato";
- dell'autocertificazione sostitutiva dello stesso

Inoltre non sussiste conseguentemente alcun obbligo di riportare nella Relazione sulla gestione degli amministratori, allegata al bilancio d'esercizio, i relativi riferimenti

La Sicurezza Informatica per la norma ISO 27001

- Le Norme ISO 27001 definiscono la Sicurezza Informatica (Information Security) come protezione di:
- Riservatezza: garantire che l'informazione sia accessibile solamente da parte delle persone autorizzate;
- Integrità: garantire l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
- Disponibilità: garantire che gli utenti autorizzati abbiano accesso all'informazione e ai beni associati quando da essi richiesto.

La valutazione del rischio

Non possiamo garantire la sicurezza se non conosciamo:

- Cosa proteggere
- Da chi e da cosa
- Quanto tempo e risorse investire per un'adeguata protezione

VALUTARE I RISCHI

Una volta conosciuti i rischi possiamo valutare e pianificare, le procedure e i dispositivi tecnici per ridurre il rischio.

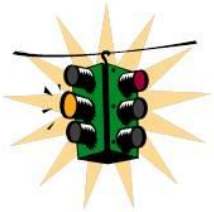
Valutazione del rischio

Rischio = f (Asset , Minacce, Vulnerabilità)

Asset : Qualunque elemento che abbia un valore nel garantire la Business Continuity

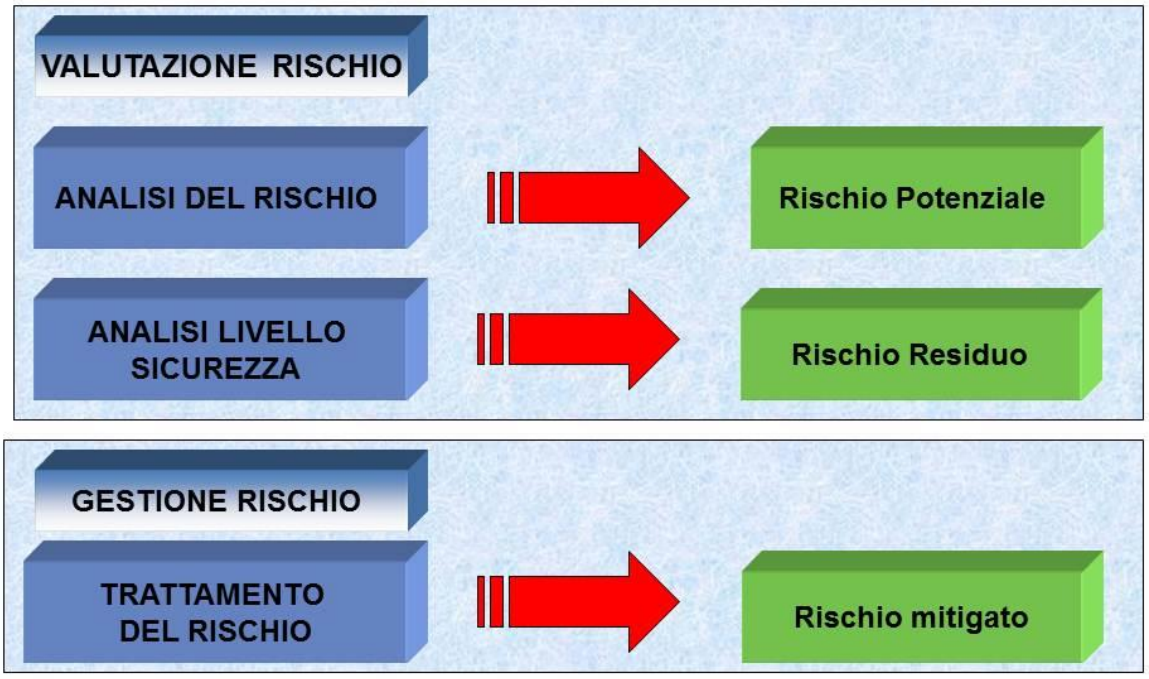
Minacce: Ogni azione o evento che può pregiudicare la sicurezza

- **Forza maggiore**
- **Carenze organizzative**
- **Errore umano**
- **Carenze tecniche**
- **Atti deliberati**



Vulnerabilità: La vulnerabilità è una debolezza [del sistema] che può essere attivata accidentalmente o sfruttata intenzionalmente.

Valutazione e gestione del rischio



Grado di sicurezza richiesto

- La sicurezza assoluta NON esiste;
- Un rischio residuo è sempre presente;
- Qual'è il livello di rischio residuo accettabile?

Decidere sulla sicurezza

Definire il livello di sicurezza (livello di rischio) per :

- gestire la continuità del servizio;
- rispettare i requisiti legali, statuti, regolamenti e requisiti contrattuali;
- tutelare e incrementare il patrimonio aziendale;
- rispondere agli incidenti.

La Sicurezza è un processo continuo

- Si devono effettuare aggiornamenti periodici sui rischi e sui controlli implementati in modo da:
- considerare i cambiamenti dei requisiti di business;
- considerare le evoluzioni tecnologiche e organizzative;
- considerare le nuove minacce e le nuove vulnerabilità;
- verificare l'efficacia dei controlli implementati.

La Sicurezza riguarda tutti

La sicurezza dei dati e delle informazioni è una responsabilità di tutto il personale a tutti i livelli dell'organizzazione.

- FORMAZIONE
- CONSAPEVOLEZZA
- COMPETENZA

Impatto dovuto alla “non sicurezza”

- Perdite economico/finanziarie
- Livelli di servizio /continuità operativa
- Riservatezza informazioni
- Immagine/credibilità
- Leggi cogenti / vincoli contrattual

Il Sistema di Gestione della sicurezza

POLITICHE AZIENDALI

Definire l'ambito del Sistema
Definire Politica di Sicurezza
Identificazione e analisi del rischio
Definire il trattamento del rischio (*accettare, diminuire, trasferire)*

Revisione del sistema di gestione
Revisione obiettivi
Programmi di miglioramento

Organizzazione
Processi
Tecnologie
Persone
Controlli

Conformità a:
- **requisiti di legge**
- **Politica di sicurezza**
- **alle norme**

Sistema Sicurezza: ISO 27001

Da BS7799 a ISO 27001

- 1993: Code of Practice
- 1995: BS 7799:1 "Code of Practice for Information Security Management "
- 1998: BS 7799:2 "Specification for Information Security Management Systems"
- 1999: aggiornamento dello standard
- 2000: ISO 17799 (parte I dei BS7799)
- 2002: BS 7799-2
- 2005: ISO/IEC 17799 - Code of Practice for Information Security Management
- 2005: ISO/IEC 27001 - Information Security Management Systems"

La norma ISO 27001:2005

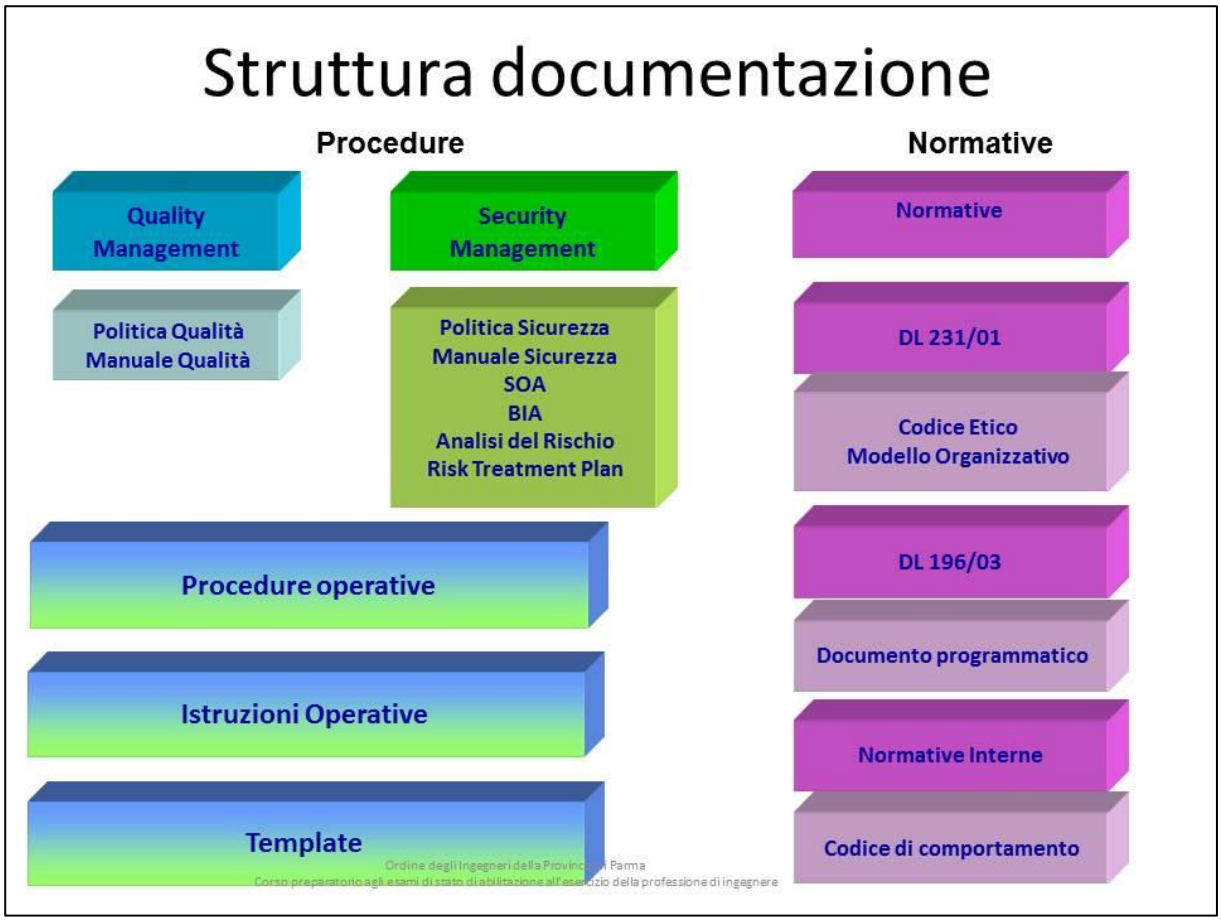
4. SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
Stabilire il SGSI
Attuare e condurre il SGSI
Monitorare e riesaminare il SGSI
Mantenere attivo, aggiornato e migliorare il SGSI
Requisiti relativi alla documentazione
Tenuta sotto controllo dei documenti
Tenuta sotto controllo delle registrazioni
5. RESPONSABILITÀ DELLA DIREZIONE
Impegno della direzione
Messa a disposizione delle risorse
Formazione e addestramento, consapevolezza e competenza
6. AUDIT INTERNI DEL SGSI
7. RIESAME DEL SGSI DA PARTE DELLA DIREZIONE
Elementi in ingresso per il riesame
Elementi in uscita dal riesame
8. MIGLIORAMENTO DEL SGSI
Miglioramento continuo
Azioni correttive e preventive

La norma ISO 27001:2005

ALLEGATO A : OBIETTIVI DI CONTROLLO E CONTROLLI

5. Politica per la sicurezza
6. Organizzazione della sicurezza delle informazioni
7. Gestione dei beni
8. Sicurezza delle risorse umane
9. Sicurezza fisica e ambientale
10. Gestione delle comunicazioni e dell'operatività
11. Controllo degli accessi
12. Acquisizione, sviluppo e manutenzione dei sistemi informativi
13. *Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti*
14. Gestione della continuità operativa
15. *Conformità (prescrizioni legali , politiche, norme di sicurezza e conformità tecnica)*

La documentazione



Struttura documentazione

Quality Management
Manuale della Qualità

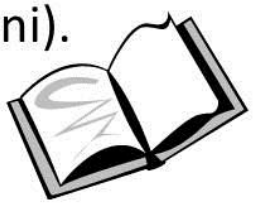
Security Management
Manuale della Sicurezza, Business Impact Analisys , Analisi dei Rischi , Risk Treatment Plan, Statement of Applicability

Procedure Operative
Servizio di Controllo Accessi e Allarmi, Sistemi e dispositivi Antivirus, Accesso Logico, Accesso Fisico, Gestione della Sala Macchine, Erogazione, Monitoraggio e Assistenza del Servizio, …

Istruzioni operative
Piano Qualità per Prg di Sviluppo e Manutenzione SW, Piano Qualità per Prg di Consulenza, Formazione e Avviamento, Piano Qualità PEC/CA, Piano Qualità per progetti Tecnologici, Piano Qualità per progetti Facility Management, Adempimenti Legali, Guida all'utilizzo dei template, …

Manuale di Qualità

- E' il documento guida in cui sono descritte le responsabilità e le modalità operative di gestione dei processi rispetto ai requisiti della norma ISO 9001
- Ove necessario rimanda alla documentazione più specifica (procedure e istruzioni).
- Contiene la Politica della Qualità



Manuale di Sicurezza

- E' il documento guida in cui sono descritte le responsabilità e le modalità operative di gestione dei processi in relazione alla sicurezza delle informazioni .
- Ove necessario rimanda alla documentazione più specifica (procedure e istruzioni).
- Contiene la Politica della Sicurezza

Codice di comportamento

Scopo del Codice è indicare gli standard di comportamento ai quali i dipendenti, funzionari ed amministratori devono attenersi.

Gli standard di comportamento si fondano su:

- comportamento eticamente corretto e conforme alle leggi;
- lealtà nei confronti dell'azienda;
- correttezza e rispetto nei rapporti tra colleghi;
- rispetto degli interessi di ogni altro interlocutore (clienti, partner commerciali, autorità governative e pubblico) e dell'ambiente;
- professionalità e diligenza professionale.

Il Codice si applica a tutte le attività ed è alla base di tutte le policy, le linee guida e le norme, presenti e future.

Protezione e uso corretto degli strumenti di lavoro

- PC fissi e portatili
- Dispositivi removibili e/o non sorvegliati
- Posto di lavoro
- Posta Elettronica
- Internet
- Dischi di rete
- Antivirus

Utilizzo strumenti di lavoro
personal computer

- Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC (es. disabilitazione screen saver temporizzato)
- Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
- Le informazioni archiviate in locale sul personal Computer, devono essere esclusivamente quelle necessarie all'attività lavorativa e tutelate con opportuni salvataggi.
- Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Aziendale.
- Durante il trasporto di PC portatili al di fuori dell’azienda, occorre mettere in atto tutte le accortezze per salvaguardare il bene da possibili danneggiamenti e/o eventuali furti e/o accessi non autorizzati.
- E’ opportuno attivare la funzione specifica (Drive Lock) per rendere illeggibile il disco fisso.
- I PC possono essere riutilizzati e/o dismessi solo se le informazioni contenute non siano intelligibili e/o ricostruibili

Utilizzo strumenti di lavoro

Dispositivi non sorvegliati

L'utente, è tenuto ad impedire qualsiasi accesso al sistema con il proprio codice identificativo, e quindi dovrà, in sua assenza:

- chiudere tutte le sessioni di lavoro attive o disconnettersi dal sistema
- adottare altri mezzi di protezione di primo livello, quali la sospensione dell'utente o l'attivazione di screen saver

Politiche di ordine del posto di lavoro

L'utente è tenuto a ridurre i rischi di accesso non autorizzato alle informazioni durante e fuori dell'orario di lavoro mediante :

- Conservazione di supporti cartacei o magnetici quando non utilizzati in contenitori dotati di sistemi di protezione (es.serratura)
- Conservare informazioni critiche in contenitori protetti (es. cassaforti ignifughe)
- Prelevare i documenti dalle stampanti e/o fax subito dopo la stampa

Utilizzo strumenti di lavoro

Utilizzo di Dispositivi removibili

- Rientrano in questa categoria chiavi hardware USB,smart card e relativi lettori, CD ecc..
- Durante il trasporto di dispositivo removibili al di fuori dell'azienda, occorre mettere in atto tutte le accortezze per salvaguardare il bene da possibili rotture e/o eventuali furti.
- Nel caso di memorizzazione dei dati riservati su tali supporti e' necessario attivare tutte le precauzioni di archiviazione.
- Distruggere o cancellare in modo sicuro i supporti di memorizzazione che contengono informazioni riservate. Questa operazione deve essere effettuata utilizzando modalità non standard del Sistema Operativo.

Utilizzo dei dischi di rete

- Sui dischi di rete devono essere presenti solamente informazioni attinenti l'attività aziendale senza vincoli di riservatezza.
- Se occorre archiviare informazioni riservate o confidenziali è necessario proteggere le singole cartelle mediante la definizione di profili di accesso e/o i singoli file con password di accesso.

Utilizzo strumenti di lavoro

Uso della posta elettronica

- Per la posta elettronica spedita all'esterno bisogna fare attenzione a non infrangere le norme di sicurezza , infatti Internet utilizza una rete pubblica sulla quale devono transitare solamente informazioni di carattere "pubblico.
- E' vietato inviare le informazioni presenti nel Sistema Informativo ad indirizzi e-mail raggiungibili attraverso la rete Internet; mentre ciò è possibile per le comunicazioni inviate ai clienti che condividono l'Intranet, in quanto le informazioni viaggiano su una rete privata e viene eseguito dal gestore di posta l'encrypting dei dati inoltrati.
- L'utilizzo della Posta elettronica da parte delle singole persone, nelle comunicazioni ai clienti e ai fornitori è da considerarsi una comunicazione "informale", intendendo come tale una comunicazione che non comporta obblighi da parte dell'azienda nei confronti del destinatario
- Tali comunicazioni devono seguire un iter ad hoc (gestito dall'Ufficio Segreteria) e sono sottoposte a livelli formali di autorizzazione.

Utilizzo strumenti di lavoro

Uso della rete Internet

- Durante gli orari di lavoro è assolutamente proibita la navigazione internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
- Non possono essere utilizzati modem privati per il collegamento alla rete.
- E' vietato portare sulle postazioni di lavoro aziendale software non regolarmente licenziato; in ogni caso, ciascun dipendente è responsabile del software presente sulla propria postazione di lavoro.
- Si raccomanda di non eseguire download di documenti da siti Web o Ftp non conosciuti
- Il servizio preposto alla Sicurezza deve essere incaricato di effettuare i controlli sul corretto utilizzo della rete internet .

Utilizzo strumenti di lavoro

Antivirus e protezione da programmi pericolosi

- Le informazioni ed i dati devono essere protetti contro il rischio di intrusione e l'azione di programmi maligni mediante l'attivazione di idonei strumenti elettronici automatici costantemente aggiornati con periodicità definita .
- Gli utenti non devono disinstallare o disattivare i prodotti antivirus dai posti di lavoro
- Qualora si sospetti la presenza di virus sulla propria postazione, occorre avvisare la funzione aziendale preposta
- Quando vengono rilevate nuove forme di virus, tutti gli utenti ne sono informati con la comunicazione delle contromisure da adottare

Linee Guida Comportamentali

Accesso fisico

- Ad ogni Dipendente viene rilasciato un badge personale di cui e' responsabile, programmato come accessi e tempi in relazione alle mansioni da ciascuno svolte
- Al momento del rilascio del badge personale il Dipendente deve sottoscrivere un documento nel quale, assieme alle caratteristiche del badge, vengono indicate: le norme di utilizzo, le eventuali responsabilità, le istruzioni in caso di smarrimento, ecc.
- Le richieste estemporanee di accesso al di fuori delle fasce orarie consentite devono essere autorizzate dal Capo Area.
- In caso di dimenticanza il Dipendente deve richiedere un badge sostitutivo temporaneo da restituire alla reception all'uscita.
- In caso di perdita il Dipendente deve informare l'Ufficio HR che provvede alla consegna di un nuovo badge e alle comunicazioni per la disabilitazione del vecchio.

Linee Guida Comportamentali

Accesso ai sistemi

Utenti - Identificazione - Validazione - Password

- Gli utenti sono identificati mediante user-id rilasciate dall'Ufficio Sicurezza
- Ogni user-id ha associato uno o più profili abilitativi che esplicitano quale e' il suo ambito di operatività'
- Ad ogni user-id e' associata una password personale e riservata utilizzata dal sistema per l'autenticazione dell'utente.

Linee Guida Comportamentali

Accesso ai sistemi

Utilizzo Password

- L'utente dovrà assicurare la segretezza ed integrità della propria password, non dovrà comunicarla a terzi.
- L'utente dovrà scegliere password "robuste", ovvero non facilmente riconducibili alla persona titolare, con un minimo di 8 caratteri alfanumerici e non potrà riutilizzarla per un certo periodo (history = 13) .
- La password personale dovrà essere sostituita ad intervalli regolari (30 gg); dopo 30gg di inattività o dopo 4 tentativi di password errata verrà bloccata .
- E' fatto tassativo divieto a tutti gli utenti:
  - di trascrivere o annotare la propria password in modo evidente o visibile;
  - di memorizzarla in processi di logon automatici;
  - di accedere al sistema di autorizzazione utilizzando codice identificativo e password di un altro utente, o di consentire che altri vi accedano utilizzando le proprie credenziali.
- La password costituisce l'elemento di autenticazione personale, qualsiasi attività sarà attribuita dal sistema al nome dell'utente il cui codice identificativo ha ottenuto l'accesso ai dati

La certificazione

Il punto di vista dell'auditor

L'auditor verifica:

- La presenza delle regole e la conformita' alle norme di riferimento;
- La conoscenza e applicazione sistematica delle regole

L'auditor valuta:

- Le evidenze oggettive (interviste, osservazioni delle attivita', documenti, registrazioni)

Tecnica:

- Campionamento

Evidenze oggettive

APPROCCIO BASATO SULL'EVIDENZA:
Il metodo razionale per raggiungere le conclusioni è *verificabile e si basa su una raccolta a campione delle informazioni disponibili.*

RISULTANZE DELL'AUDIT (AUDIT FINDINGS)
Risultati della valutazione delle evidenze raccolte rispetto ai criteri di audit

Evidenze oggettive : fonti di informazioni

Le **fonti di informazioni** scelte possono variare con il campo e con la complessità dell'audit e possono comprendere:

a) Interviste con impiegati e con altre persone;
b) Osservazioni di attività e delle condizioni e dell'ambiente di lavoro circostante;
c) Documenti, quali politica, obiettivi, piani, procedure, norme, istruzioni, licenze e permessi, specifiche, contratti ed ordini;
d) Registrazioni di ispezioni, resoconti di riunioni, rapporti di audit, registrazioni di supporto;
e) Rapporti da altre fonti, ad esempio, informazioni di ritorno dal cliente , altre informazioni pertinenti da parti esterne e valutazioni di fornitori;

Evidenze oggettive : fonti di informazioni

Le interviste sono uno dei mezzi importanti di raccolta di informazioni e sono eseguite in maniera adattiva alla situazione ed alla persona intervistata.

Tuttavia, l'auditor prende in considerazione quanto segue:

a) Le interviste sono rivolte a persone di opportuni livelli e funzioni che eseguono attività o compiti nell'ambito del campo dell'audit;
b) L'intervista è condotta sul luogo di lavoro abituale della persona che viene intervistata;
c) Le interviste possono iniziare con la richiesta di descrivere il lavoro svolto;
d) Le interviste possono proseguire con le richiesta di evidenze puntuali ed oggettive a documentazione delle attività effettuate.

Firma elettronica, firma elettronica qualificata, firma digitale

A cosa servono

È qualcosa di più che un semplice “copia e incolla” dell’immagine della tua firma nel documento di testo.
Il software di firma lega la firma a un documento specifico e, proprio come gli esperti sono in grado di rilevare un documento cartaceo che è stato modificato dopo essere firmato, il software di firma è in grado di rilevare una modifica ad un file firmato in modo elettronico.

Firma elettronica

Per firma elettronica la legge intende l'insieme dei dati in forma elettronica, allegati ovvero connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica qualificata

La firma elettronica qualificata è una firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità sia certificata da un certificato qualificato emesso da una **Certificate Authority** o **Certification Authority** (CA) ovvero da un *trusted third party* in conformità alla normativa europea e nazionale.

Firma digitale

La firma digitale, è una particolare specie di "firma elettronica qualificata", basata sulla tecnologia della crittografia a chiavi asimmetriche.

Crittografia asimmetrica

Diversamente dalle “chiavi” di crittografia simmetriche , cioè uguali tra mittente e destinatario, la crittografia asimmetrica si basa invece su chiavi diverse:

- chiave “privata” posseduta dal solo detentore dell’identità
- chiave “pubblica” nota a tutti.

Nota: Algoritmi matematici di recente scoperta (RSA) permettono di decrittare positivamente con la chiave “pubblica” solo i messaggi correttamente generati con chiave “privata”.
I “certificati digitali” rilasciati dalle società di CA assegnano la chiave “privata” (ad es. su un supporto USB) e forniscono pubblicamente la chiave “pubblica” (ad es. tramite accesso via internet)

Un esempio

La firma digitale garantisce che un file non sia stato alterato, come se fosse stato chiuso in una busta sigillata.

- La firma è una “sintesi” (*digest*) del file ottenuto con un processo ciclico (si pensi, a puro titolo di esempio, all’ultimo carattere del codice fiscale)
- Il *digest* viene criptato e spedito insieme al file.
- Il destinatario decifra il *digest* inviato e lo controlla col *digest* ottenuto da un ricalcolo sul file ricevuto.
- Se i *digest* corrispondono, è dimostrata l’integrità del file ovvero l’assenza di manomissioni.

Vediamo l'esempio passo passo:

1. Una donna vuole inviare un messaggio con **firma elettronica** ad un uomo.

2. Dapprima calcola il *digest* del suo messaggio di testo, poi usando la chiave privata fornita dalla CA, codifica il *digest*, trasformandolo in una **firma digitale**.

3. La firma ed il messaggio sono trasmessi insieme.

4. Utilizzando la chiave pubblica della donna ottenuta via internet dalla CA, l'uomo decifra la firma ottenendo il *digest* originale.

5. A questo punto ricalcola il *digest* dal messaggio di testo ricevuto

6. La corrispondenza di *digest* garantisce l'integrità del messaggio.

Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici

"Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici - significa fornire al mittente, dal parte del proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione

Allo stesso modo, quando il messaggio perviene al destinatario, il server del gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale.

Cosa viene certificato

Con un messaggio inviato tramite servizio di posta elettronica certificata si ottiene:

- Autenticazione del mittente (provenienza certa del messaggio)
- Autenticità del contenuto del messaggio (sia in termini di correttezza formale cioè assenza da virus, sia in termini di garanzia del contenuto e assenza di alterazione durante la trasmissione)
- Avvenuta/mancata ricezione del messaggio da parte del provider del destinatario
- Marcatura temporale opponibile a terzi.

Elementi di sicurezza

Ricevuta di accettazione:	Contiene i dati di certificazione del gestore del mittente quale prova dell'avvenuta spedizione
Ricevuta di avvenuta consegna	Costituisce prova della consegna del messaggio all'indirizzo elettronico dichiarato dal destinatario. Contiene i dati di certificazione che certificano il momento della consegna. Viene emessa unicamente a seguito di valida ricezione della busta di trasporto
Avviso di mancata consegna	Comunicato al mittente entro 24 ore dall'invio

Tutto questo Indipendentemente dall'effettiva lettura del messaggio.

Posta elettronica e PEC

Nella posta elettronica il documento informatico trasmesso per via telematica si intende **inviato** e **pervenuto** al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato
Nella Posta elettronica certificata Il documento informatico trasmesso per via telematica si intende **spedito** dal Mittente se inviato al proprio gestore, e si intende **consegnato** al destinatario quando è reso disponibile all'indirizzo elettronico da questi dichiarato e, più precisamente, nella casella di posta elettronica certificata messa a disposizione dal gestore

Ricevute e buste di trasporto

- Sono sottoscritte con firma digitale al fine di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute e dei messaggi di posta elettronica certificata
- Ciascun messaggio è contrassegnato da un riferimento temporale
- I log dei gestori sono contrassegnati quotidianamente da marca temporale
- I gestori assicurano i livelli di servizio

- I Gestori non accettano messaggi con Virus Informatici, nel caso avvisano il mittente tempestivamente e non danno corso alla trasmissione o consegna
- I Gestori conservano il messaggio e la traccia informatica delle operazioni svolte per 30 mesi

PostaCertificat@: l'offerta PEC dellaPubblica Amministrazione

Numero richieste attivazione da portale: **1.244.883** Valori aggiornati al 13/05/2012

Cos'è PostaCertificat@:
La PostaCertificat@ è un servizio gratuito che consente ai cittadini di dialogare con le Pubbliche Amministrazioni dotate di PEC presenti nell'Indirizzario PA del Portale.

Perché attivarla
Per eseguire comodamente via internet numerose operazioni, come richiedere informazioni, inviare istanze e documentazioni, ricevere documenti e comunicazioni senza doversi recare fisicamente negli uffici della Pubblica Amministrazione.

I servizi gratuiti e a pagamento per il cittadino
Oltre alla casella PostaCertificat@, è possibile usufruire gratuitamente di altri Servizi Base (Fascicolo, Indirizzario delle Pubbliche Amministrazioni, Notifica su posta elettronica tradizionale) e attivare, a pagamento, i Servizi Avanzati quali Firma Digitale, Calendario degli Eventi e Servizio di Notifica con SMS.

Decreto del presidente del consiglio dei ministri
Il Decreto del Presidente del Consiglio dei Ministri del 6 maggio 2009 stabilisce che, a ciascun cittadino che ne faccia richiesta, il "Dipartimento per la digitalizzazione della Pubblica Amministrazione e per l'innovazione tecnologica" assegni a titolo non oneroso un indirizzo di Posta Elettronica Certificata, da utilizzare per tutte le comunicazioni con la Pubblica Amministrazione.

Per approfondimenti consulta:
- le pagine di www.postacertificata.gov.it

Carta identità elettronica

La carta d'identità elettronica è strumento di identificazione personale nonché di autenticazione per l'accesso ai servizi web erogati dalle Pubbliche Amministrazioni. come previsto dal Codice dell'Amministrazione Digitale.
La sperimentazione del documento è stata avviata nel 2000 con un progetto nato da un'iniziativa del Ministero dell'Interno in collaborazione con 156 Comuni.
Terminata la fase di sperimentazione, la carta d'identità elettronica sarà operativa per tutti i cittadini. Le regole tecniche del nuovo documento di riconoscimento personale sono state indicate nel Decreto Interministeriale dell'8 novembre 2007.

Il documento di riconoscimento elettronico contiene tutti i identificativi e le informazioni ufficiali relative alla persona e funzion anche come carta di servizi.

La Carta è una smart card che contiene, memorizzate su un microch su una banda ottica:

- i dati personali,
- il codice fiscale,
- i dati di residenza,
- la cittadinanza,
- il codice numerico del comune di rilascio,
- la data del rilascio,
- la data di scadenza,
- la firma del titolare,
- la fotografia,
- eventuale indicazione di non validità ai fini dell'espatrio.

Potrà contenere anche i dati amministrativi del Servizio Sanitario Nazionale, e tutte le informazioni occorrenti per la firma digitale.

Al momento del rilascio della carta a tutela della sicurezza del cittadino sono rilasciate allo stesso tre codici personali segreti:

PIN: una sequenza di numeri personali e segreti che permette il riconoscimento dell'utente in tutta sicurezza;

PUK: il codice per sbloccare il PIN nel caso in cui il cittadino ne sbagli la digitazione per tre volte o dimentichi il proprio numero;

CIP: per impedire l'uso del PIN ad altri se la carta viene smarrita o rubata e garantire la propria privacy.

Il Centro Nazionale dei Servizi Demografici (CNSD) presso il Ministero dell'Interno, assicura e garantisce la gestione unitaria del sistema di emissione della CIE, la sua piena funzionalità e la trasparenza e sicurezza dei processi di autenticazione e convalida dell'informazioni anagrafiche.

Carta Nazionale dei Servizi (CNS)

La Carta Nazionale dei Servizi, ovvero le Carte Regionali dei Servizi create secondo lo standard CNS, è lo strumento attraverso il quale i cittadini vengono riconosciuti in rete in modo certo e possono usufruire dei servizi erogati in via telematica dalle Pubbliche amministrazioni in attesa della Carta d'identità Elettronica
Si tratta di una smart card con microchip che contiene i dati identificativi della persona (nome, cognome,codice fiscale), il certificato di autenticazione che, in combinazione con il PIN fornito dall'Ente emettitore consente l'autenticazione in rete, e può contenere anche il certificato di firma digitale.
A differenza della Carta d'identità elettronica, non contiene la foto del titolare e pertanto non può essere usata come documento di riconoscimento "a vista" ma consente forme più flessibili e veloci di produzione ed erogazione.

Servizi sono offerti da

- Agenzia Entrate
- Avvocatura Generale dello Stato
- Azienda Provinciale per i Servizi Sanitari di Trento
- Azienda Ospedaliera Universitaria 'San Martino'
- DigitPA - Ente Nazionale Per La Digitalizzazione Della Pubblica Amministrazione
- Garante protezione dati personali
- Guardia di Finanza - Comando Generale
- INAIL - Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro
- Innovazione Italia
- INPS - Istituto Nazionale Previdenza Sociale
- Istituto Zooprofilattico dell'Abruzzo e del Molise 'G. Caporale'
- Ministero degli Affari Esteri
- Ministero Economia e Finanze
- Regione Abruzzo
- Regione Basilicata
- Regione Calabria
- Regione Campania
- Regione Emilia-Romagna
- Regione Friuli Venzia Giulia
- Regione Liguria
- Regione Molise
- Regione Puglia
- Regione Sardegna
- Regione Sicilia
- Regione Veneto
- …

La Carta sanitaria elettronica

Svolge più funzioni contemporaneamente:

- CNS (da attivare)
- Tessera sanitaria nazionale (TS)
- Tessera europea di assicurazione malattia (Team) sostituisce il modello E-111 e garantisce l'assistenza sanitaria nell'Unione Europea e in Norvegia, Islanda, Liechtenstein e Svizzera, secondo le normative dei singoli paesi
- Tesserino del codice fiscale
- Chiave privata di accesso al fascicolo sanitario elettronico che contiene i dati sanitari personali
- …

Per attivare la carta il cittadino si dovrà recare presso uno degli sportelli abilitati presenti nella regione di appartenenza, portando con se la carta sanitaria e un documento di identità valido. L'operatore allo sportello procede all'attivazione della carta e rilascia al cittadino i codici di accesso PIN e PUK ed il codice di identificazione CIP (opzionale). Per poter accedere ai servizi on-line messi a disposizione dalla Pubblica Amministrazione, il cittadino si dovrà munire di un apposito lettore di smart card e del relativo software di gestione.

Sui siti delle Regioni sono disponibili:

- manuale operativo concernente gli aspetti organizzativo e funzionale del ciclo di vita della TS-CNS;
- elenco degli sportelli regionali abilitati per l'attivazione delle CNS;
- i requisiti tecnici minimi necessari per l'utilizzo della TS-CNS;
- il pacchetto software di gestione della TS-CNS e le relative istruzioni per l'installazione;
- manuale utente per l'utilizzo della carta.

Per approfondimenti consulta:

- le pagine del DigitPA www.digitpa.gov.it/carta-nazionale-dei-servizi
- il sito del progetto CNS www.progettocns.it

Il progetto CNS | Home

www.progettocns.it

My MSN | Google | Gmail: l'email di Go... | Rodeo Houston Radio | NETGEAR Router M... | Free Online Dictionary | Nanda&Leo | Other bookmarks

CNS Carta Nazionale dei Servizi

Home | Amministrazione

› Il Progetto CNS

La Carta Nazionale dei Servizi (CNS) è una smart card per accedere ai servizi online della Pubblica Amministrazione su tutto il territorio nazionale. E' lo strumento fondamentale per rendere immediatamente fruibili i servizi già in rete e per accelerarne la diffusione. La CNS è una straordinaria innovazione per una nuova e più efficace interazione tra cittadino e Pubblica Amministrazione.

› Come usare la carta

La CNS va opportunamente inserita nell'apposito lettore collegato al proprio PC, direttamente da casa o dall'ufficio oppure presso gli sportelli polifunzionali dislocati sul territorio e viene attivata attraverso la digitazione del codice numerico personale.

Corso completo all'utilizzo della CNS:parte 1 e parte 2

› Quali servizi

La CNS, come strumento operativo tra cittadino e Pubblica Amministrazione, permette oltre alle funzionalità di firma digitale tutti i servizi resi disponibili dalle diverse amministrazioni tra cui i pagamenti on line, la tessera sanitaria, il codice fiscale.

›Aggiornamento certificati di firma

Area riservata (l'accesso richiede l'autenticazione tramite la propria carta CNS) dedicata agli aggiornamenti dei certificati di firma.

Istruzioni standard per l'aggiornamento dei certificati di firma.

(PDF 860 KB, luglio 2011)

› Quali Amministrazioni

Le Pubbliche Amministrazioni che hanno aderito al contratto quadro messo a disposizione dal DigitPA per l'emissione di CNS al fine di agevolare lo sviluppo delle iniziative e i vantaggi e le opportunità connesse all'utilizzo della Carta Nazionale dei Servizi.

› Area tecnica

Area dedicata agli "sviluppatori ed integratori" per rispondere alle più comuni problematiche e dubbi sui vari aspetti del sistema delle CNS.

› File Protector

Area riservata (l'accesso richiede l'autenticazione tramite la propria carta CNS) dedicata agli aggiornamenti del software di firma e cifratura File Protector.

Istruzioni per l'aggiornamento di File Protector.

(ZIP 1,2 MB, febbraio 2011)

Ricerca

Cerca

Kit per il cittadino

› Istruzioni e software per l'utilizzo della CNS

FAQ

› Un aiuto per iniziare

Call Center - tel. 02 688 25 561

› Per i titolari di CNS e per le amministrazioni

Link utili

› I www di riferimento

Mappa | Glossario | Utilità | Note Legali e Privacy

Copyright ©

W3C XHTML 1.0 | W3C CSS

Codice dell'Amministrazione Digitale (CAD)

Il decreto legislativo 30 dicembre 2010, n. 235recante il testo del **nuovo Codice dell'Amministrazione Digitale** (CAD) è entrato in vigore dal 25 gennaio 2011 (G.U. n. 6 del 10 gennaio 2011, n. 6 – SO n. 8), apportando modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82.
Il nuovo CAD, aggiornando la normativa di riferimento, rappresenta il pilastro su cui si basa il processo di rinnovamento della Pubblica Amministrazione, avviato con l'approvazione del decreto legislativo n. 150/2009 (c.d. riforma Brunetta), che ha introdotto nella PA i principi di meritocrazia, premialità, trasparenza e responsabilizzazione dei dirigenti.
In questa sezione sono disponibili le principali informazioni che riguardano gli enti locali ed, in particolare, si segnalano i riferimenti normativi e le novità relative al CAD.

Il decreto crescita 2.0 modifica il CAD

Il decreto legge 179/2012, convertito con modificazioni in legge 221/2012, ha introdotto nuove modifiche al testo vigente del CAD. In particolare si evidenziano i seguenti nuovi obblighi:

- l'inserimento dei requisiti tecnici di accessibilità all'art 57 su moduli e formulari;
- l'ampliamento dell'indice degli indirizzi delle pubbliche amministrazioni ai gestori dei pubblici servizi nell'art. 57bis;
- l'ulteriore modifica all'art. 68, dedicato all'analisi comparativa delle soluzioni informatiche, stilando un elenco di soluzioni che le PA devono adottare per acquisire programmi informatici o parti di essi.

Le nuove disposizioni per la modulistica tipo

L'articolo 57 del CAD, così modificato dall'art. 9, comma 6, lettera e), legge 221/2012, prevede che:

1. Le pubbliche amministrazioni provvedono a definire e a **rendere disponibili per via telematica, nel rispetto dei requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari** validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.
2. **Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati**; in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli o formulari. La mancata pubblicazione è altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili.

Ciò significa che gli enti locali sono tenuti a pubblicare sul sito i modelli tipo o un collegamento diretto ai **modelli tipo CELVA**, in caso contrario sono obbligati ad accettare qualsiasi modello venga presentato.

Il decreto spending review modifica il CAD

Il decreto legge 95/2012, convertito con modificazioni dalla legge 135/2012, ha introdotto ulteriori modifiche al testo vigente del CAD ed, in particolare, ha previsto con l'art. 19, comma 7:

- l'abrogazione dei commi 3-bis, 3-ter, 3-quater, 3-quinquies, 3-sexies, 3-septies e 3-octies dell'articolo 15 del CAD (istituiti con il decreto legge 5/2012), in merito alla gestione in forma associata delle funzioni ICT.

Con la legge 135/2012 vengono quindi **abrogate le recenti indicazioni inserite nel CAD, riportando la gestione associata dell'ICT alle funzioni fondamentali nell'art. 14, comma 28**, del decreto legge 78/2010, convertito con modificazioni dalla legge 122/2010, così modificato appunto dall'art. 19, comma 1 della legge 135/2012.
Il decreto sviluppo modifica il CAD

Il decreto legge 83/2012, recante "Misure urgenti per la crescita del Paese", convertito con modificazioni dalla legge 134/2012, ha introdotto invece le seguenti modifiche:

- l'istituzione dell'**Agenzia per l'Italia digitale** e la soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione;
- la sostituzione del comma 1 dell'art. 68 in merito all'**acquisizione di programmi informatici.**

Il decreto semplificazioni modifica il CAD

Il decreto legge 5/2012, convertito con modificazioni in legge 35/2012, ha introdotto alcune modifiche al testo vigente del CAD. In particolare si evidenziano i seguenti nuovi obblighi:

- la pubblicazione sul sito web istituzionale da parte delle pubbliche amministrazioni del codice IBAN e dei dati necessari da indicare obbligatoriamente nella causale di versamento;
- l'erogazione dei servizi esclusivamente tramite i canali telematici, compresa la posta elettronica certificata, a partire dal 1° gennaio 2014.

Di seguito si allegano i documenti principali sul nuovo CAD, disponibili anche sul sito web del Ministero della pubblica amministrazione e la semplificazione.

Principi Guidaguida del nuovo CAD

Sancire nuovi diritti, nuove opportunità, nuovi doveri:

- **Diritto all' uso delle tecnologie verso amministrazioni e gestori di servizi pubblici (art.3)**
  I cittadini e le imprese hanno diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Non sarà più possibile quindi per un'amministrazione o per un gestore di pubblico servizio obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale sicuro (nella maggior parte dei casi costituito dalla PEC – Posta Elettronica Certificata), certificato e con piena validità giuridica che permetta di dialogare con la PA dal proprio computer. Il nuovo codice amplia questo diritto anche verso i gestori di servizi pubblici. Il complesso della riforma della PA permette poi di esigere questo diritto anche mediante l'uso dell'azione collettiva e introduce l'effettiva disponibilità degli strumenti necessari nella valutazione dei dirigenti e delle organizzazioni
- **Opportunità per le amministrazioni di capitalizzare il "dividendo dell'efficienza" che l'innovazione digitale consente (art.15)**
  I risparmi ottenuti attraverso l'innovazione tecnologica e organizzativa (reingegnerizzazione dei processi) dovranno essere effettivamente misurati e andranno in parte ad incentivare il personale interessato, secondo le norme del d.lgs. 150/09, in parte a finanziare nuova innovazione.
- **Obbligo di coordinarsi, di lavorare insieme, di fare sistema (art.14)**
  L'amministrazione digitale non può lavorare a compartimenti stagni: se lo Sato ha l'obbligo del coordinamento dell'intero sistema, il nuovo codice impone alle regioni di promuovere un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso con le autonomie locali e dà il compito allo Stato di favorire la collaborazione interregionale .
  Dare chiarezza, validità e strumenti operativi all'innovazione:
- **Più stringente definizione della validità dei documenti e dei procedimenti (art.20-23-quater)**
  Un'intera sezione del nuovo CAD, profondamente rivisitata rispetto alla vecchia versione, si propone di diradare l'incertezza sul complesso processo di dematerializzazione dei documenti. Le regole del nuovo codice rendono effettivamente praticabile l'obiettivo di una PA senza carta.
- **Maggiore sostenibilità organizzativa per l'innovazione (art.17)**
  L'innovazione non si fa da sola: richiede di essere sostenuta da una robusta organizzazione: il codice impone a tutte le amministrazioni centrali (e suggerisce alle regioni e agli Enti locali) di

costituire una nuova posizione di dirigente generale responsabile in toto dei processi di informatizzazione e crea una Conferenza perché questi soggetti si parlino, si confrontino, imparino a collaborare tra loro.

- **Collegamento stretto con il ciclo della performance e la valutazione del merito (art.12)**
  L'attuazione delle disposizioni del CAD è comunque rilevante ai fini della misurazione e della valutazione della performance organizzativa e individuale dei dirigenti. Alle opportunità si accompagnano quindi sia gli incentivi, sia le sanzioni. L'innovazione diventa per la prima volta materia di valutazione del personale, da cui dipendono sanzioni ed incentivi.

Ora si può fare

Nella Pubblica Amministrazione digitale i cittadini e le imprese hanno nuovi diritti che il codice precisa e definisce e che rende quindi effettivamente esigibili, essi sono basati su strumenti che aiutano anche le amministrazioni a lavorare meglio e a spendere meno:

- **I pagamenti elettronici (art.5)**
  Già il codice del 2005 imponeva alle amministrazioni di consentire i pagamenti ad esse spettanti con le tecnologie digitali, ma non diceva come. Il nuovo CAD prevede una serie di strumenti operativi (ad es. le carte di credito) e consente di avvalersi di soggetti anche privati per la riscossione, aprendo di fatto un nuovo mercato dei servizi.
- **Le comunicazioni tra imprese e amministrazioni (art.5 bis)**
  Il digitale diventa la regola nei rapporti tra imprese ed amministrazioni e il cartaceo l'eccezione. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.
- **La PEC: canale di comunicazione e semplice strumento di identificazione (articoli 6 e 65)**
  La PEC (Posta Elettronica Certificata) diventa, per tutte le imprese e i professionisti,che per legge devono esserne dotati e per i cittadini che lo desiderano il mezzo più veloce, sicuro e valido per comunicare con le amministrazioni pubbliche. Da lì passano comunicazioni, atti e provvedimenti, ma anche istanze e dichiarazioni che un cittadino può trasmettere usando la propria casella PEC anche come strumento di identificazione che può evitare, nella maggior parte dei casi, l'uso della firma digitale.
- **La validità dei documenti è indipendente dal supporto (articoli 20-23 quater)**
  Nella sezione I del Capo II vengono descritte dettagliatamente le condizioni validità dei documenti informatici, dei passaggi da analogico a digitale e viceversa, introducendo tra l'altro un semplice sistema di contrassegno generato elettronicamente e stampato direttamente dal cittadino dal proprio computer, per sancire la conformità dei documenti cartacei a quelli digitali (c.d. glifo). La dematerializzazione, come sappiamo, riguarda sia la produzione direttamente digitale degli atti, sia la digitalizzazione di quelli che erano stati prodotti in forma analogica (su carta), per entrambi i procedimenti mancavano certezze di validità che ora il nuovo CAD detta, lascando poi ad un successivo documento l'effettiva implementazione delle norme tecniche
- **Conservazione digitale dei documenti: meno carta, senza perdere né sicurezza né storia (articoli 43-44 bis)**
  In centinaia di chilometri di archivi giace l'immenso patrimonio informativo della PA: sino ad ora per digitalizzare un documento senza conservarne l'originale cartaceo era necessaria una certificazione uno ad uno. Ora un responsabile della conservazione può certificare il processo di digitalizzazione e di conservazione servendosi se vuole di "conservatori" accreditati. anche privati. E' così possibile risparmiare milioni di metri cubi di spazio e rendere possibile la reperibilità dei documenti. E' ovviamente fatta salva l'integrità cartacea di particolati

documenti dotati di valore storico, culturale o artistico che potranno essere meglio conservati, anche perché non annegati tra milioni di faldoni.

- **Le nuove frontiere della sicurezza digitale (art.51)**
  Se la PA diventa digitale la sicurezza dei dati, dei sistemi e delle infrastrutture è sempre più un obiettivo chiave, anche per costruire quella fiducia nei servizi pubblici online che ancora manca. Il codice introduce disposizioni importanti sia sulla continuità operativa, sia sul disaster recovery dettando le modalità per il coordinamento delle azioni delle singole amministrazioni e per la predisposizione di piani operativi
- **La sfida degli open data (articoli 52 e 68)**
  Il nuovo CAD mette in primo piano la responsabilità della amministrazioninell'aggiornare, divulgare e permettere la valorizzazione dei dati pubblici secondo i principi del cosiddetto "open government". In particolare le pubbliche amministrazioni, al fine di valorizzare e rendere fruibili i dati pubblici di cui sono titolari, promuovono progetti di elaborazione e di diffusione degli stessi anche attraverso l'uso di strumenti di finanza di progetto, assicurando la gratuità dell'accesso e la pubblicazione dei dati in formato aperto in modo che possano essere rielaborabili da terzi.
- **I servizi online (articoli 54 e 63-65)**
  Le amministrazioni pubbliche sono tenute a dar conto dei servizi online che hanno messo a disposizione di cittadini ed imprese sia sul proprio sito istituzionale, sia dandone notizia al Dipartimento della Funzione Pubblica. La sezione III del V Capo del codice definisce con maggiore concretezza le norme già presenti nel CAD del 2005: le pubbliche amministrazioni e i gestori di servizi pubblici progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente. E' previsto poi una più ampia possibilità di accesso ai servizi che si basa sia sulla Carta d'Identità elettronica e carta dei servizi sia su altri strumenti che comunque consentano l'individuazione del soggetto che richiede il servizio
- **Dare voce ai cittadini anche su Internet (art.54 e 63)**
  La cosiddetta "riforma Brunetta" ha tra i suoi cardini l'empowerment dei cittadini accrescendo le occasioni di dar loro voce possibilità di esprimere giudizi sulla soddisfazione nella fruizione dei servizi. Anche per i servizi online vale lo stesso principio: le amministrazioni sono tenute ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti.
- **Moduli e formulari sempre disponibili (art.57)**
  Il codice si mette dalla parte dei cittadini e delle imprese che non possono perdere tempo nella ricerca spesso vana di moduli e formulari. Le pubbliche amministrazioni devono provvedere a definire e a rendere disponibili per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà. Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati; in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli o formulari. La mancata pubblicazione è altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili.
- **Far viaggiare le informazioni e non le persone e non chiedere ai cittadini quello che le amministrazioni sanno già (art. 58)**
  E' una delle richieste più pressanti di cittadini ed imprese: che la PA non richieda loro dati che già possiede. Il CAD rende possibile lasciare in pace i cittadini prevedendo l'obbligo per le amministrazioni tenutarie di banche dati di predisporre apposite convenzioni aperte alla adesione di tutte le amministrazioni e volte a disciplinare le modalità di accesso ai dati senza oneri a loro carico. Il principio era già presente nel CAD del 2005, ma ancora una volta il nuovo

CAD indica lo strumento e le sue regole, ne impone poi l'obbligatorietà prevedendo, in caso di inadempienza la nomina di un commissario ad acta che intervenga a predisporre le convenzioni e quindi in ultima analisi a tutelare il diritto degli utenti.

- **Siti pubblici e trasparenza (art. 54)**
  Già il d.lgs 150/09 detta stringenti principi per la trasparenza delle amministrazioni pubbliche verso una "total disclosure" che vede nei siti internet pubblici il principale strumento di pubblicità. La successiva direttiva 105 della Commissione Indipendente per la Valutazione, Integrità e Trasparenza della PA (Civit) elenca con precisione quali sono i dati e le notixie che ciascuna amministrazione deve inserire nel sito Internet. Ora il Codice completa il quadro indicando l'obbligo per le amministrazioni di tenere aggiornati i dati (e considerando questo aspetto nella valutazione di dirigenti) e di trasmetterne una cospicua parte al Dipartimento della Funzione Pubblica che potrà così avere una conoscenza diretta e utilizzabile di molti fenomeni, a partire ad es. dalla consistenza dei servizi online presenti. Il codice introduce poi l'obbligo di pubblicare sui siti pubblici in modo integrale tutti i bandi di concorso.
- **Il patrimonio informativo delle amministrazioni e le basi di dati di interesse nazionale (art.60)**
  Il nuovo codice ripropone la definizione del 2005 di "basi di dati di interesse nazionale" - che costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate – ma rende operativa questa nozione cominciando ad indicare quali sono:
  a) repertorio nazionale dei dati territoriali;
  b) indice nazionale delle anagrafi;
  c) banca dati nazionale dei contratti pubblici di cui all'articolo;
  d) casellario giudiziale;
  e) registro delle imprese;
  f) gli archivi automatizzati in materia di immigrazione e di asilo.
  In questo ambito particolare importanza riveste la banca dati dei contratti pubblici, sia per la ricchezza di informazioni che può dare sulla spesa pubblica, sia al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e della prevenzione di fenomeni di corruzione.
- **Le regole tecniche (art. 71)**
  Per molti dei provvedimenti previsti dal nuovo codice sarà necessario predisporre regole tecniche che saranno dettate da appositi decreti del Presidente del Consiglio dei Ministri. Per gran parte di queste l'organo tecnico competente è DigitPa che istituirà tavoli di lavoro e di consultazione con tutti gli stakeholders pubblici e privati interessati, con particolare attenzione per le imprese di ICT .

I tempi di applicazione

La complessa normativa prevista dal Codice richiede tempi ragionevoli per il loro recepimento, per adeguare processi e per formare il personale. La riforma entrerà in vigore quindi a scaglioni secondo una precisa tempistica che coincide comunque con gli impegni presi nel piano di e-gov 2012.

- **Entro 3 mesi:**
  Le pubbliche amministrazioni utilizzeranno la posta elettronica certificata o altre soluzioni tecnologiche per tutte le comunicazioni che richiedono una ricevuta di consegna ai soggetti che hanno preventivamente dichiarato il proprio indirizzo
- **Entro 4 mesi:**
  Le amministrazioni individueranno un unico ufficio responsabile dell'attività ICT
- **Entro 6 mesi:**

- Le PA centrali pubblicheranno sui propri siti istituzionali i bandi di concorso e tutta una serie di informazioni sul proprio funzionamento nell'ottica della *total disclosure*
- Le amministrazioni consentiranno ovunque i pagamenti ad esse spettanti per via telematica
- Le amministrazioni e le imprese comunicheranno tra loro esclusivamente per via telematica

- **Entro 12 mesi:**
  - Saranno emanate le regole tecniche che consentiranno di dare piena validità alle firme elettroniche diverse da quella digitale, nonché alle copie cartacee e, soprattutto, a quelle digitali dei documenti informatici, dando così piena effettività al processo di dematerializzazione dei documenti della PA
  - Saranno emanate le regole tecniche per la conservazione sostitutiva dei documenti in forma digitale dando il via agli archivi informatizzati
  - Le pubbliche amministrazioni non potranno richiedere l'uso di moduli e formulari che non siano stati pubblicati sui propri siti istituzionali
  - Il cittadino fornirà una sola volta i propri dati alla pubblica amministrazione. Sarà onere delle amministrazioni (in possesso dei dati) assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre amministrazioni richiedenti
  - Saranno definite le basi di dati di interesse nazionale
  - Saranno emanate tutte le regole tecniche previste dal CAD
  - Le regole del nuovo CAD si applicheranno, mediante un apposito DPCM, anche alla Presidenza del Consiglio dei Ministri e all'Amministrazione finanziaria
- **Entro 15 mesi:**

  Le PA predisporranno appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività

Glossario del Codice dell'Amministrazione digitale

ALLINEAMENTO DEI DATI: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

AMMINISTRAZIONI CERTIFICANTI: le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni;

AMMINISTRAZIONI PROCEDENTI: le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio;

AUTENTICAZIONE DEL DOCUMENTO INFORMATICO: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

AUTENTICAZIONE DI SOTTOSCRIZIONE: l'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione e' stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive;

CARTA D'IDENTITÀ ELETTRONICA: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

CARTA NAZIONALE DEI SERVIZI: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

CERTIFICATI ELETTRONICI: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

CERTIFICATO: il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche;

CERTIFICATO QUALIFICATO: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

CERTIFICATORE: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

CHIAVE PRIVATA: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

CHIAVE PUBBLICA: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

COPIA INFORMATICA DI DOCUMENTO ANALOGICO: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

COPIA INFORMATICA DI DOCUMENTO INFORMATICO: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

COPIA PER IMMAGINE SU SUPPORTO INFORMATICO DI DOCUMENTO ANALOGICO: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

DATO A CONOSCIBILITÀ LIMITATA: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

DATO DELLE PUBBLICHE AMMINISTRAZIONI: il dato formato, o comunque trattato da una pubblica amministrazione;

DATO PUBBLICO: il dato conoscibile da chiunque;

DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA': il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal presente testo unico;

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE: il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato;

DISPONIBILITÀ: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;

DOCUMENTO AMMINISTRATIVO: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Le relative modalità di trasmissione sono quelle indicate al capo II, sezione III, del presente testo unico;

DOCUMENTO ANALOGICO: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

DOCUMENTO DI RICONOSCIMENTO: ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare;

DOCUMENTO D'IDENTITA' ELETTRONICO: il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età;

DOCUMENTO D'IDENTITA': la carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare;

DOCUMENTO INFORMATICO: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

DUPLICATO INFORMATICO: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

FIRMA DIGITALE: 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;

FIRMA ELETTRONICA: 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: 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: 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;

FRUIBILITÀ DI UN DATO: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

GESTIONE DEI DOCUMENTI: l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa e' effettuata mediante sistemi informativi autorizzati;

GESTIONE INFORMATICA DEI DOCUMENTI: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;

GESTORE DI POSTA ELETTRONICA CERTIFICATA: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;

IDENTIFICAZIONE INFORMATICA: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

LEGALIZZAZIONE DI FIRMA: l'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa;

LEGALIZZAZIONE DI FOTOGRAFIA: l'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato;

ORIGINALI NON UNICI: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

POSTA ELETTRONICA CERTIFICATA: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

PUBBLICHE AMMINISTRAZIONI CENTRALI: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI: l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti;

TITOLARE: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

VALIDAZIONE TEMPORALE: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Diritto d’autore sul software

Principi generali

La tutela del software trova fondamento nel Decreto legislativo 518/92, la cui introduzione si è tradotta nella modifica della legge 22 aprile 1941, n 633 sul Diritto d'Autore ("l.d.a.").

Ambito della tutela

Sono protetti in base a questa legge "i programmi per elaboratore, in qualsiasi forma espressi, purchè originali quali risultato di creazione intellettuale dell'autore. […] Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso" (art. 2, n. 8, l.d.a.).

Il termine deve essere inteso nel senso di ricomprendere tutte le forme di programma, pertanto sia quelle percepibili dall'uomo (programma-sorgente) che quelle leggibili da parte di una macchina (programma-oggetto). Sono parimenti assoggettate alla tutela in questione le parti del programma incorporate nell'hardware stesso (firmware e software di base), in forma permanente o rimovibile.

La tutela d'autore viene inoltre estesa al materiale preparatorio per la progettazione del programma stesso, compresi i "diagrammi di flusso", che rappresentano graficamente la sequenza delle operazioni che il programma deve compiere - e che, dunque, ne esprimono, seppure in forma sintetica, l'intera costruzione - e i "diagrammi a blocchi", che costituiscono lo sviluppo dei precedenti (articolo 2 l.d.a., cit.). Tale materiale può tuttavia ricevere tutela solo se completo, nel senso di consentire la realizzazione del programma in una fase successiva" (Direttiva n. 250/91 sulla protezione dei programmi per elaboratore elettronico, 7° considerando).

In questa prospettiva non è proteggibile il materiale che contiene solo una traccia di lavoro per il programmatore, come è ad esempio la descrizione, analisi e scomposizione in sottoproblemi elementari del problema al quale il programma deve dare soluzione, (c.d. metodo top-down).

Dato il tenore dell'articolo 2, n. 8 l.d.a., non sono oggetto della protezione i manuali d'uso o manutenzione del programma che tuttavia, in quanto ne ricorrano i presupposti, potranno essere tutelati secondo i principi generali del diritto d'autore e comunque, qualora contengano anche la riproduzione di parti sostanziali del programma, tali parti sono protette dal diritto d'autore sul programma medesimo.

L'originalità richiesta, perché il programma sia proteggibile secondo lo schema del copyright, consiste nell'avere il suo ideatore pensato e sviluppato il programma autonomamente, senza averlo - e questo basta - copiato da altri.

Fondamento del diritto

Il diritto d'autore sul software che soddisfi i requisiti sopra indicati sorge per il fatto stesso della creazione di tale prodotto informatico, quindi automaticamente al momento dell'incorporazione dell'opera nel supporto materiale che ne permette l'individuazione, e non è subordinato all'adempimento di alcuna formalità di deposito o di registrazione. Esiste comunque, presso la SIAE, un registro pubblico speciale dei programmi per elaboratore la cui funzione è quella di fissare la data di deposito del programma (artt. 103 e 105 l.d.a).

Essendo la registrazione facoltativa, essa serve essenzialmente a determinare la priorità dell'esclusiva d'autore, specie per quei programmi che non si vogliono immediatamente commercializzare.

Facoltà del titolare

Il titolare del programma dispone di tutta una serie di facoltà di uso e sfruttamento economico dei prodotti informatici.

La prima delle attività riservate è costituita dalla facoltà di riproduzione del programma, permanente o temporanea, totale o parziale, con qualsiasi mezzo o in qualsiasi forma (articolo 64 bis, lett. a) l.d.a.).
Ancora, il titolare del software ha facoltà di traduzione, adattamento, trasformazione e ogni altra modificazione del programma, nonché di riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma (articolo 64 bis, lett. b) l.d.a.).
Di tali facoltà il titolare del software può disporre, in tutto o in parte, mediante la conclusione di contratti di cessione, licenza, vendita di esemplari o licenza d'uso del programma.
Se all'utente interessa soltanto una facoltà di uso del software, il titolare del software potrà concedere una licenza d'uso non esclusiva o vendere un esemplare del programma. Se all'utente interessa ottenere il possesso del software e facoltà di sfruttamento commerciale dello stesso, il titolare potrà concedere una licenza esclusiva sul programma ovvero cedere a titolo definitivo i diritti patrimoniali sul software.

Contenuto

Si è detto, in proposito del requisito della creatività del software, quanto sia difficile stabilire - nei casi concreti - se, rispetto a prodotti già sviluppati, il programma consista in un'elaborazione talmente creativa da costituire opera autonoma (in cui il nucleo originale precedente è riconoscibile unicamente quale traccia o "spunto"), un'elaborazione comunque sufficientemente creativa da costituire opera derivata ovvero una mera riproduzione di un programma altrui con varianti secondarie e non funzionali dell'opera originaria, e quindi contraffazione. Una delle particolarità del software è rappresentata dalla normale non definitività dell'opera stessa. Un programma, per essere utilmente utilizzato, può richiedere di essere continuamente modificato, aggiornato, e questa trasformazione evolutiva può spingersi fino a troncare ogni legame con il software originario. Ciò comporta ovviamente non poche conseguenze sul piano giuridico.

Originalità dell'opera

Per quanto concerne la facoltà del titolare di un diritto d'autore di trasformare ed elaborare l'opera originaria - facoltà questa prevista in via generale dagli articoli 4 e 18 l.d.a. e, con riferimento specifico al software, dall'articolo 64 bis, lett. b), l.d.a. - si pone la questione circa i criteri per l'accertamento di un'elaborazione sufficientemente creativa da costituire opera derivata (e non mera riproduzione con varianti dell'opera originaria) ovvero un'elaborazione talmente creativa da costituire opera autonoma, in cui il nucleo originale precedente è riconoscibile unicamente quale traccia o "spunto" (Cfr. Trib. Milano, 13 marzo 1997, in Riv. Dir. Ind. 1988, II, 290).
La distinzione non è di scarsa importanza.
La semplice riproduzione di un'opera originaria con varianti da parte di un terzo, infatti, non determina il sorgere di un nucleo di originalità meritevole di autonoma tutela d'autore; in questo caso la riproduzione da parte del terzo costituisce violazione del diritto d'autore originario. L'autore dell'opera derivata può godere, invece, di un distinto diritto d'autore, anche se nei limiti dell'elaborazione che la distingue dall'opera originale. Il suo autore incontra inoltre, nell'esercizio dei suoi diritti, l'ostacolo rappresentato dalla necessità di una previa autorizzazione dell'autore dell'opera originaria alla modificazione, elaborazione e trasformazione dell'opera stessa.
Diversamente in caso di opera autonoma, questa potrà considerarsi a tutti gli effetti "originaria" e non abbisognare pertanto di alcun consenso da parte dell'autore dell'opera precedente, da cui pure ha derivato la traccia.

Contraffazione

Nell'odierna produzione tecnologica è sempre più rara l'innovazione completamente indipendente dallo "state of the art" in essere, come dimostra la frequente difficoltà di una analoga distinzione anche nel campo brevettuale, fra la mera contraffazione evolutiva ed il ritrovato relativamente

nuovo ma dipendente dall'attuazione di un'idea precedente (anch'esso tutelabile previo consenso del titolare di quest'ultima: articoli 2587 cod. civ. e 5 R.D 1127/1939 "Legge Invenzioni"). Opera derivata può essere la traduzione, la trasformazione da una forma all'altra di una precedente opera, può consistere nelle modificazioni od aggiunte che costituiscano un rifacimento sostanziale dell'opera originaria (che possono anche essere localizzate solo in alcuni punti e non necessariamente riguardare l'intera opera originaria), può risolversi in adattamenti, riduzioni, compendi, variazioni non costitutive opera originale.
Come si vede, la casistica delle possibili variazioni è molto vasta ed alcune ipotesi si adattano perfettamente alle derivazioni cui può essere soggetto un software (traduzioni da un linguaggio ad un altro, modificazioni al fine di rendere il prodotto compatibile con altro sistema operativo, nuove versioni; senza contare le "personalizzazioni": c.d. "customizing" effettuate da programmatori terzi o dagli stessi utenti nei confronti del software originario già legittimamente acquistato). Tanto è vero che il legislatore italiano, quando nel 1992 ha novellato la legge sul diritto d'autore introducendo le disposizioni relative alla tutela giuridica del software (D. Lgs. 518/1992 attuativo della Direttiva CEE 91/250), ha previsto espressamente che i diritti esclusivi conferiti sui programmi per elaboratore comprendono anche il diritto di effettuare o autorizzare "la traduzione, adattamento, la trasformazione e ogni altra modificazione del programma per elaboratore, nonché la riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma" (articolo 64 bis, lett. b) l.d.a.). Il consenso per una data forma di elaborazione, d'altra parte, non vale anche per altre, e non vale per lo sfruttamento commerciale dell'opera derivata. Se l'autore dell'elaborazione è un soggetto diverso rispetto al titolare dell'opera originaria, occorre il consenso del titolare del diritto sull'opera originaria per "utilizzare economicamente il nuovo lavoro" (Cass. n. 9139/1990).
Stabilire se un software modificato sia riconducibile ad un'opera derivata piuttosto che autonoma è comunque un esame essenzialmente tecnico, non collegato a valutazioni giuridiche od economiche. In linea di massima si dovrà procedere ad una comparazione strutturale tra i due programmi, tenendo conto dell'algoritmo complessivo e delle distinte procedure indipendenti in esso contenute. Nonostante la molteplicità delle concrete fattispecie, al cui esame dovrà necessariamente essere verificata la comparazione di fatto delle opere, sotto il profilo di diritto rileva l'indispensabile accertamento circa la riconoscibilità qualitativa (e non meramente quantitativa) dell'opera originaria nell'opera derivata.
In altri termini, mentre la derivazione della maggior parte dell'algoritmo tutelabile osta inevitabilmente ad un'elaborazione sufficientemente creativa per costituire un'opera originaria anche sotto il profilo qualitativo (integrandosi al massimo una modificazione, protetta nei limiti delle modifiche apportate), la derivazione di alcune sequenze protette dell'algoritmo - elaborate secondo ulteriori scelte di combinazione o di composizione informatica - non sembra escludere la sufficiente autonomia dell'opera, qualora sia diverso ed indipendente il procedimento creativo di risoluzione attuato dal programmatore successivo. La comparazione strutturale dovrà effettuarsi pertanto tenendosi conto, attraverso i successivi livelli di astrazione, non solamente dell'algoritmo complessivo, ma delle distinte procedure indipendenti in esso contenute (interacting sub-routines).
Ne consegue che - mentre la diversa successione di procedure, già compiute ed autonome all'interno del programma, non sembra idonea a configurare una modificazione sottratta al necessario consenso dell'autore precedente - la diversa combinazione di singoli comandi o di istruzioni originali già presenti nel programma anteriore può essere in grado di dare luogo a nuove procedure, complessivamente dotate di creatività originaria. Conformemente a quanto si è sopra sostenuto, per conseguire un'opera informatica originaria risultano - al contrario - tendenzialmente irrilevanti eventuali elaborazioni della sola rappresentazione grafica, visualizzata sul monitor o stampata su carta (c.d. "look and feel"), trattandosi di mere trasposizioni formali del codice sorgente sulla cui struttura deve attuarsi l'astrazione comparativa complessiva.

La tutela giuridica

Gli strumenti di tutela del diritto di autore sui software nelle ipotesi di illecita riproduzione ovvero illecita elaborazione o trasposizione in diversa forma del programma senza l'autorizzazione del titolare, consistono in azioni giudiziarie - esperibili anche in via di urgenza - dirette:

all'accertamento del diritto violato ed all'inibizione dell'attività illegittima (articolo 156 l.d.a.);

alla rimozione o alla distruzione degli esemplari frutto di tale ultima attività (articolo 158 l.d.a.);

alla condanna al risarcimento del danno (articolo 158 l.d.a.);

alla pubblicazione della decisione in una o più giornali a spese della parte soccombente. Tale sanzione può peraltro essere ordinata dal giudice su istanza di parte o anche d'ufficio (articolo 166 l.d.a.).

Altra forma di violazione del diritto d'autore sui programmi è infine il plagio, inteso quale violazione del diritto morale di paternità dell'opera.

Categorie di software

Software libero
Il software libero (*free software*) è software distribuito in modo che chiunque ne abbia il permesso di uso, copia e distribuzione, in forma modificata o meno, gratis o a pagamento. In particolare, ciò significa che il codice sorgente deve essere disponibile: «Senza il sorgente non è software».
Ci sono molti modi diversi per rendere un programma libero e molte questioni di dettaglio, che possono essere risolte in più di un modo e nondimeno rendere "libero" un programma.
Il software libero è una questione di libertà, non di prezzo. Ma aziende di software propietario talvolta usano il termine *free software* per riferirsi al prezzo[1]. Alcune volte ciò significa che si può ottenere una copia del binario senza pagarlo; altre volte significa che una copia è inclusa nel computer che si sta comprando.
A causa di questa potenziale confusione, quando una azienda di software dice di produrre *free software*, bisogna sempre controllare le licenze per verificare se gli utenti hanno effettivamente tutte le libertà che il software libero implica. Talvolta è software libero, altre volte no.

Software *open source*
Il termine *open source* software è usato da alcuni più o meno con lo stesso significato di software libero. Meglio usare il termine "software libero".

Software di dominio pubblico
Il software di pubblico dominio (*public domain*) è software privo di copyright. È un caso speciale di software libero senza permesso d'autore, il che significa che alcune copie o versioni modificate possono non essere affatto libere.
Talvolta si usa il termine "dominio pubblico" in un'accezione vaga per intendere "libero" o "disponibile gratuitamente". Tuttavia "di dominio pubblico" è un termine legale che significa precisamente "senza copyright". Per chiarezza, meglio usare "di dominio pubblico" solo con questo significato, e usare altri termini per intendere gli altri significati.

Software con permesso d'autore
Il software con permesso d'autore[2] (copyleft) è software libero le cui condizioni di distribuzione non permettono ai ridistributori di porre alcuna restrizione addizionale all'atto di ridistribuire o modificare il software. Questo significa che ogni copia del software, anche se modificata, deve essere software libero.
Il permesso d'autore è un concetto generale; per utilizzarlo effettivamente per un programma, bisogna usare dei precisi termini di distribuzione, e ci sono molti modi di scrivere dei termini di distribuzione per il permesso d'autore.

Software libero senza permesso d'autore
L'autore di software libero senza permesso d'autore (*non–copylefted free software*) dà il permesso di ridistribuire e modificare il programma, e anche di aggiungervi ulteriori restrizioni.
Se un programma è libero, ma non ha permesso d'autore, alcune copie o versioni modificate possono non essere affatto libere. Un'azienda di software può compilare il programma, con o senza modifiche, e distribuire il file eseguibile come un prodotto software proprietario.
Software semilibero

---

[1] il termine *free* in inglese significa sia gratuito che libero.
[2] si tratta di un gioco di parole, che qui viene reso con "permesso di autore": *copyright* (diritto di autore) è formato dalle parola *copy* (copia) e *right* (diritto, ma anche destra), opposto di *left* (sinistra, ma anche lasciato).

Il software semilibero (*semi-free software*) è software non libero, ma che è distribuito col permesso per i privati di essere usato, copiato, distribuito e modificato (incluse le versioni distribuite con modifiche) senza scopo di lucro.

Software proprietario

Il software proprietario (*proprietary software*) è quello che non è libero o semilibero. Il suo utilizzo, la ridistribuzione o modifica sono proibiti o richiedono un permesso o sono sottoposti a tali vincoli che in pratica non si possono fare liberamente.
Attenzione agli abusi pubblicitari del termine proprietario - *proprietary* che negli anni '80 e '90 indicava il software non IBM e negli anni dal 2000 in poi il software non Microsoft o ultimamente anche non Google o Apple essendo usato in una metafora di "non pubbico" o "non universalmente riconosciuto".

Freeware

Il termine *freeware* non ha una definizione comunemente accettata, ma è comunemente utilizzato per i pacchetti software che possono essere ridistributi ma non modificati (ed il loro codice sorgente non è disponibile). Questi pacchetti non sono software libero, perciò non usate *freeware* per indicare il software libero.

Shareware

Lo *shareware* è software che dà la possibilità di ridistribuire copie, ma impone a chiunque continui ad usarne una copia di pagarne la licenza d'uso.
Lo *shareware* non è software libero, nè semilibero perché, per la maggior parte dei casi, il codice non è disponibile (pertanto, non è assolutamente possibile modificare il programma) ed inoltre non è distribuito con il permesso di farne una copia ed installarlo senza pagare una licenza d'uso, neanche per chi lo utilizzi per un'attività senza fini di lucro.
In pratica, molti ignorano i termini di distribuzione e lo usa comunque, ma le licenze d'uso non lo permettono.

Software Commerciale

Il software commerciale è software sviluppato da un'azienda allo scopo di guadagnare dal suo uso. "commerciale" e "proprietario" non sono la stessa cosa! La maggior parte del software commerciale è proprietario, ma c'è software libero commerciale, e c'è software non commerciale non libero.

Principi relativi alle intrusioni nei sistemi informatici.

Rischi di una intrusione

I rischi associati all'accesso non autorizzato al sistema informativo comprendono perdite economiche, furto di informazioni sensibili (personali o industriali), perdita di immagine aziendale o perdita di controllo dei sistemi informativi stessi.

Alcune delle possibili mancanze di sicurezza, nell'accesso ai sistemi informativi e alle reti, possono riguardare:

- la rete Internet e gli altri punti di accesso elettronico, partendo da tecnologie implementate quali firewall, VPN, websites, ecc;
- i modelli procedurali, inclusa l'interazione umana (Social Engineering, Physical Intrusion, ecc.);
- gli accessi fisici, con particolare attenzione verso la sicurezza degli archivi e della documentazione, eventi naturali (power failure, incendi, allagamenti).

Gli attacchi e le vulnerabilità

Per attacco si intende generalmente il tentativo di "hacking" del sistema/i.

Tipologie di attacco

Internet

L'attacco condotto da Internet ha come oggetto dell'attacco i servizi pubblici dell'azienda (es. Mail, Web, Ftp, Dns, Firewall).

I rischi connessi sono:
- i dati aziendali possono essere rubati o modificati;
- i sistemi critici possono essere compromessi;

i motivi di debolezza possono essere:
- la rete non disegnata correttamente;
- i sistemi non configurati correttamente;
- il firewall non configurato correttamente.

Gli scenari possibili sono due:
- l'attacco è condotto da hacker esterni che tuttavia potrebbero - anche solo temporaneamente - aver avuto accesso alla rete interna;
- l'attacco è condotto da utenti legittimi dell'Azienda (es: dipendenti, consulenti) in grado di ottenere l'accesso alla rete aziendale e/o a funzioni critiche del sistema informativo.

Statisticamente questo ultimo tipo di attacco è estremamente diffuso (abuso di privilegi) e pericoloso (utenti interni disonesti conoscerebbero la locazione dei dati critici e saprebbero monetizzarne più facilmente una relativa violazione).

War-dialing

L'attività di wardialing consiste nell'effettuare un test di accesso alle linee telefoniche aziendali al fine di identificare apparecchiature (modem, fax, centralini, ecc.) non autorizzati o male configurati.
La protezione, svolta dai sistemi di difesa perimetrale (Firewall, ecc.), risulterebbe di fatto annullata se un hacker riuscisse a connettersi ad un modem allacciato ad un computer in rete.

L'attacco telefonico o wardial consiste in diverse fasi:
- scan dello spazio telefonico e riconoscimento modem/fax/voce;
- identificazione dell'apparato connesso al modem (es: access server, unix server, RAS, ecc.);
- tentativo di accesso alla risorsa attraverso "password guessing", password di default, errori di configurazione;
- accesso alla risorsa;

Web Application

Le applicazioni web sono di norma strutture assai complesse e includono componenti software di vario tipo. Tipicamente queste risiedono sul web server, sull'application server, su database di vario genere e, infine, sui sistemi di backend aziendali.
Spesso le singole componenti dell'applicazione web sono sviluppate, supportate e mantenute da diversi attori e strutture di una stessa azienda.
Sebbene il termine "applicazione" tenda a connotare una singola entità funzionale, in realtà le applicazioni web si compongono di tanti parti di codice, spesso provenienti da differenti vendor e/o sviluppatori di terze parti.
Per questo motivo rendere sicura un'applicazione web può richiedere la completa visibilità dei flussi informativi aziendali con capacità tecniche non comuni.

Wireless

I segnali di una scheda wireless sono in grado di coprire distanze consistenti e in molti casi la copertura del segnale va oltre i confini fisici dell'Azienda.
È facile trovare Access Points Wireless del tutto insicuri e configurati inadeguatamente.
Situazioni di questo tipo permettono ad un potenziale hacker di potersi connettere alla rete Aziendale senza lasciare alcuna traccia fisica di accesso all'edificio dell'Azienda.

Provenienza dell'attacco

Secondo la provenienza dell'attacco il PenTest può essere:

esterno eseguito su reti pubbliche (TCP/IP dedicate, reti Frame Relay, telefoniche, satellitari, ecc.) o su reti private con uscita pubblica (Internet, X.25/X.121, DECnet, modem/numeri verdi, RAS, wireless, ecc.);

interno eseguito su internal LAN (via RAS o dalla LAN aziendale), LAN to LAN private, LAN to LAN pubbliche.

Attacco esterno

Prevede l'attacco alla rete di una azienda (con bersagli specificati o meno) da una o più reti esterne e può essere utilizzato in diverse modalità:

Surface mode (Network Scanning/Penetration)
L'attacco consiste nella scansione dei bersagli con diversi network e host scanneralla ricerca di vulnerabilità per ottenere l'accesso non autorizzato alla rete dell'azienda.

Advance Mode (Social Engineering + Network Scanning/Penetration)
L'attacco consiste nell'impiego delle tecniche e tecnologie adottate nel Surface Mode, nell'ottenere informazioni sensibili dalle componenti che si interfacciano con la rete bersaglio (personale interno/esterno, consulenti, fornitori, clienti, partner commerciali) enell'attacco ad eventuali network che si interfacciano con la rete bersaglio.

Total Mode (Trashing + Social Engineering + Network Scanning/Penetration)
L'attacco consiste nell'impiego delle tecniche e tecnologie adottate nel Surface e Advanced Mode, nell'ottenere informazioni sensibili attraverso l'individuazione, il recupero e l'analisi dei rifiuti aziendali provenienti dall'azienda bersaglio.

Social engineering

Il social engineering è stato definito come "l'abile manipolazione di una popolazione tramite la disinformazione al fine di ottenere un cambiamento desiderato nelle abitudini e nelle tendenze della stessa popolazione".

Nel contesto di un attacco, il social engineering é utilizzato per descrivere l'acquisizione di informazioni sensibili o di impropri accessi privilegiati ai sistemi da parte di un hacker, stabilendo ingannevole relazioni di fiducia con persone all'interno dell'organizzazione obiettivo dell'attacco.

Tali tecniche possono essere usate per ottenere fraudolentemente informazioni confidenziali, quali user-id, passwords, numeri telefonici interni, informazioni personali o qualsiasi altra informazione utile.

Attacco interno

Prevede l'attacco alla rete bersaglio da una posizione privilegiata dell'attaccante, cioè dall'interno. Si tenga presente che un malintenzionato, spesso, non si pone limiti di tempo e di tecniche (compreso il Social Engineering) per ottenere informazioni dall'interno, sempre che non abbia agganci o provenga proprio dall'interno (come avviene per la maggior parte degli attacchi).

Apparecchiature da verificare

Il caso più comune è il test di sistemi che forniscono servizi tramite Internet, come ad esempio WEB Server, Mail Server, Server di autenticazione, Commercio Elettronico, Applicazioni WEB, Apparati di rete (Router, Firewall, IDS, ecc.) o altri sistemi analoghi.

Oltre a questi tipi di sistemi, può essere utile verificare altri tipi di apparecchiature come ad esempio, sistemi interni di backup, stampanti, centralini telefonici, apparati wireless o bluetooth, ponti radio, telefoni cellulari e persino contatori dell'energia elettrica.

In sostanza, tutto quello che è attaccabile può essere oggetto di un *Penetration Test*, svolto da parsonale interno o da consulenti, modulando conseguentemente risorse, modalità, tempi e costi.

Nel caso di un numero elevato di sistemi da verificare, specie se simili, tempi e costi possono essere ridotti eseguendo controlli "a campione", cercando di trovare un compromesso ragionevole, ad esempio:

- un sub-network (la DMZ citata sopra, un singolo ufficio, fabbricato o data center, un dominio od un gruppo omogeneo di servers);
- un'applicazione con tutte le sue componenti (il sistema applicativo, il suo database, il sistema operativo sui quali risiedono e le varie
  - componenti software ed hardware a supporto);
  - un singolo componente od una famiglia di componenti di rete (il firewall, il sistema operativo "xyz" di una specifica versione, il web od il mail server, il sistema vPN od il file repository).

Rilevazione dell'intrusione e ripristino dei sistemi

Modifica delle password sui sistemi

Questa operazione, raccomandata in ogni caso, risulta indispensabile quando si rileva che un'intrusore abbia avuto accesso al password file o abbia usato un password-sniffer in grado di catturare le password utente e ritrasmetterle in chiaro sulla rete.

Reinstallazione completa dei sistemi compromessi

Nel caso in cui sia difficoltoso o troppo oneroso verificare i checksum crittografici del sistema compromesso si dovrà procedere alla reinstallazione integrale del sistema utilizzando i supporti di distribuzione originali o delle copie sicuramente conformi.

imozione dei programmi utilizzati e delle modifiche

I risultati delle analisi saranno utilizzati per individuare tutti i file utilizzati per effettuare l'intrusione e tutti i file acceduti del corso della stessa intrusione, tali file dovranno essere eliminati.

I principali punti di attenzione saranno orientati a trovare:

- Vulnerabilità conosciute del sistema o dei prodotti installati: installare le patch appropriate;
- Presenza di codice malizioso (back door, trojan horse) con funzioni sconosciute o nascoste come cancellazione di log file, avvio di servizi su porte inusuali per consentire accessi senza password o con password sconosciute all'organizzazione: reinstallare il software corrotto;
- Aggiunta di nuovi utenti alla lista degli utenti autorizzati includendo privilegi inappropriati: reinstallare una versione verificata del file di autorizzazione.
- Modifica delle password di utenti esistenti: reinstallare di una versione verificata dei file di password;
- Procedure insicure o inadeguate (p.e. per modifica di password e delle loro scadenze): rinforzare tali procedure;
- File di configurazione corrotti (p.e. contenenti servizi precedentemente disabilitati): correggere questi file;

Infine è indispensabile analizzare tutti i file che vengono eseguiti al boot del sistema per rilevare la presenza di back door, o trojan horse: reinstallare una versione verificata dei file eseguiti al boot.

Reinstallazione dei programmi eseguibili e dei file binari dai supporti di distribuzione originali.

E' necessario identificare tutti i file che sono stati aggiunti o modificati nel corso dell'intrusione poiché non è possibile determinare quali funzioni nascoste sono state attivate o quali finzioni critiche possono essere influenzate da tali modifiche. Per i file eseguibili (inclusi i file non binari come i shell script) e gli altri file binari (p.e. librerie), verificare il checksum crittografico per assicurarsi che questi file non siano compromessi.

Revisione delle configurazioni del sistema.

Dovranno essere verificati i file di configurazione del sistema che includono i seguenti tipi:
User accounts;
System services e loro configurazioni;
Strumenti di audit e monitor;
Access control list.
Si dovrà comparare tutta la configurazione del sistema con una copia fiduciaria o comparare i checksum crittografici con quelli archiviati prima dell'intrusione.

Eliminare vulnerabilità e correggerle.

Indagare sulle vulnerabilità di cui esiste documentazione o programmi presso le comunità di haker e informarsi su dove reperire soluzioni come patch o hot-fixes.

Verifica dei requisiti e della tempistica per il ritorno alla normale operatività.

E' necessaria un completa verifica dei requisiti di operatività che i sistemi assolvevano precedentemente all'intrusione, prima del ritorno in esercizio dei sistemi stessi.

Ripristino dei dati utente da un backup affidabile

Un intrusore può aver alterato i dati utente e i programmi di un'area applicativa, esempi di queste azioni possono includere:

- L'installazione di back door per futuri accessi, p.e. installando un programma in una user directory locale che viene eseguito al login utente e che attiva una shell di login non protetta che può essere acceduta da remoto;
- La compromissione dei dati utente a fini di sabotaggio anche con piccole modifiche difficilmente individuabili;

Abilitazione dei sistemi e dei servizi.
Saranno abilitati quei servizi, precedentemente disabilitati, di cui si è certi della non vulnerabilità o che siano stati opportunamente corretti.
Saranno riconnessi i sistemi ripristinati alla rete locale e nel caso la rete locale sia stata isolata questa sarà riconnessa alla rete pubblica.

Monitor in attesa di ulteriori scan o probe da parte dell'intrusore.
In molti casi è possibile raccogliere maggiori informazioni su un intrusore durante le attività preparatorie all'intrusione piuttosto che immediatamente dopo. In questi casi si rivela particolarmente utile aver installato efficaci strumenti di monitor.

Azioni conclusive

A seguito di una intrusione e del successivo ripristino della normale operatività sarà utile effettuare una analisi complessiva delle implicazioni determinate dall'evento. Questa analisi dovrà, per gli specifici aspetti, tener conto di tutte le parti coinvolte.
Dovranno, in via indicativa, essere analizzati i seguenti argomenti:

- Valutazione dell'adeguatezza degli strumenti di protezione e individuazione delle violazioni dei sistemi;
- Revisione dei piani di sicurezza, delle politiche e delle procedure;
- Revisione delle direttive ad utenti ed amministratori dei sistemi volte a prevenire ulteriori violazioni;
- Valutazione della necessità di una nuova analisi del rischio in base alla gravità degli effetti dell'intrusione;
- Aggiornamento dell'inventario dei sistemi e dei loro assetti;
- Partecipazione ad azioni investigative e legali.