Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per l'Istruzione
Direzione Generale per il personale della scuola

Assistenti Tecnici

AREA
NUOVE TECNOLOGIE

Materiali di studio

Prove selettive per la "seconda posizione economica" ex artt. 6 e 7 Accordo Nazionale M.I.U.R. - OO.SS. concernente l'attuazione dell'art.2 comma 3 della sequenza contrattuale (ex. art. 62 CCNL/2007) del 25 luglio 2008

Materiale di studio Assistenti Amministrativi – Area Nuove Tecnologie

DATABASE, LE RETI E LA MULTIMEDIALITÀ....4
1 Database e reti LAN 4
1.1 I calcolatori 4
1.2 Hardware e Software 6
1.3 Files 7
1.4 Gestire le informazioni....8
1.5 DAI FASCICOLI AI DATABASE 9
1.6 REALIZZAZIONE DI UN DATABASE....9
1.7 INSERIMENTO DATI 11
1.8 ELEMENTI DI UN DATABASE 12
1.9 RECORD e CAMPI 13
1.10 PROGETTARE UN DATABASE 14
1.11 RETI LAN 15
1.12 SERVER 17
1.13 TIPOLOGIA DI RETI 18
2 Internet e la Multimedialità 20
2.1 INTERNET 20
2.2 www, mail, ftp e gli altri protocolli d Internet 20
2.3 VoIP....21
2.4 BREVE STORIA DI INTERNET 22
2.5 WORLD WIDE WEB....23
2.6 INTERNET E MULTIMEDIALITA'....24
2.7 IL COMMERCIO ELETTRONICO 25
2.8 INTERNET PER LAVORO (ESEMPI DI POTENZIALITA') 26
2.9 E-MAIL....30
2.10 LA COMUNICAZIONE SU INTERNET, BLOG, PODCAST....31
2.11 LA FORMAZIONE ON-LINE....34
2.12 MOTORI DI RICERCA....37
2.13 RIEPILOGO 38
2.14 RESENTE E FUTURO....40
FIRMA DIGITALE E PROTOCOLLO INFORMATICO....43
1 La Firma digitale 43
1.1 FIRMA DIGITALE....43
1.2 CNIPA E FIRMA DIGITALE 44
1.3 CHIAVI ASIMMETRICHE 46
1.4 LA FUNZIONE DELLA FIRMA DIGITALE....47
1.5 COME CRIPTARE UN DOCUMENTO 48
1.6 COME USARE LA FIRMA DIGITALE....48
1.7 IMPORTANZA DELLA FIRMA DIGITALE....50
1.8 USI DELLA FIRMA....51

1.9 Firme "leggere" e firme "forti".....53
1.10 FIRMA DIGITALE E P.A.....54
VERSO UN SISTEMA INFORMATICO DELLA P.A. 55
1.Il sistema informativo della P.I.....55
1.1 CAMBIAMENTO ORGANIZZATIVO 55
1.2 TECNOLOGIE INFORMATICHE ED AUMENTO DI EFFICIENZA 56
1.3 IL VECCHIO SISTEMA INFORMATIVO 57
1.4 LE NUOVE ESIGENZE 57
1.5 DAL CENTRALISMO AL DECENTRAMENTO.....58
1.6 VANTAGGI NELL'UTILIZZO DI UN SISTEMA INFORMATIVO.....59
1.7 I LIVELLI DI UTENZA 60
1.8 INDIVIDUAZIONE DEI LIVELLI LOGICO-TERRITORIALI.....62
1.9 RETE PRIVATA DI COLLEGAMENTO 63
1.10 ARCHITETTURA DELLE DIREZIONI REGIONALI e DEI CSA 64
1.11 I POSTAZIONI DI LAVORO 64
1.12 SICUREZZA INFORMATICA 65
1.13 ARCHITETTURA DELLA RETE 66
1.14 FLUSSO ATTUALE DELLE INFORMAZIONI 66
1.15 L'ORGANIZZAZIONE DEL SERVIZIO 67
1.16 LE FUNZIONI INTEGRATE DEL SISTEMA.....68
1.17 SETTORI DI APPLICAZIONE 70
1.18 SISTEMA DI SUPPORTO ALLE DECISIONI.....70
1.19 GESTIONE GIURIDICA.....71
1.20 ORGANIZZAZIONE E AUTOMAZIONE D'UFFICIO.....72
2.La rete unitaria della P.A.....73
2.1 IL CAMBIAMENTO DELLA P.A. 73
2.2 NASCE L'AIPA 74
2.3 COMPITI DELL'AIPA.....74
2.4 IL PROGETTO PORTANTE 75
2.5 LA RETE UNITARIA 76
2.6 LO STUDIO DI FATTIBILITA'.....77
2.7 BREVE STORIA 82
2.8 AIPA - CNIPA 83
2.9 SPC - Sistema Pubblico di Connettività 85
2.10 DI Scuola 86
2.11 SIDI Learn 91
2.12 SISTEMA INFORMATIVO UNITARIO DELLE AMMINISTRAZIONI PUBBLICHE.....93
2.13 A REINGEGNERIZZAZIONE DEI PROCESSI 94
2.14 RETE E AUTONOMIA LOCALE.....96
2.15 E PORTE DELLA RETE 96
2.16 RINCIPALI AREE DI INTERVENTO.....96
2.17 SERVIZI PER IL TRASPORTO.....97
2.18 SERVIZI PER LA COOPERAZIONE 97
2.19 SERVIZI PER LA COOPERAZIONE APPLICATIVA.....98
2.20 CONDIVIDERE LE INFORMAZIONI 98

2.21 L'ORGANIZZAZIONE DEL SERVIZIO 98
2.22 LINEE GUIDA 99
2.23 CENTRO TECNICO 99
2.24 CENTRO DI GESTIONE.....100
2.25 FIGURE INTERESSATE.....101
2.26 PIANO TRIENNALE.....101
2.27 PIANO TRIENNALE 2007-2009.....102
2.28 POSTA CERTIFICATA.....105
2.29 ROTOCOLLO INFORMATICO 106
2.30 FIRMA DIGITALE.....106

3. La sicurezza informatica 107
3.1 IL FATTORE SICUREZZA.....107
3.2 INTERVENTI.....107
3.3 RISCHI.....108
3.4 SISTEMA INFORMATIVO SICURO 108
3.5 NORMATIVA E SICUREZZA 109
3.6 PRINCIPALI NORMATIVE 111
3.7 PIANO DELLA SICUREZZA 112
3.8 ANALISI DEI RISCHI.....112
3.9 POLITICHE DELLA SICUREZZA 116
3.10 GESTIONE DEL RISCHIO 118
3.11 IL PIANO OPERATIVO 119
3.12 SICUREZZA FISICA E SICUREZZA LOGICA.....119
3.13 CONTROLLO DEGLI ACCESSI ANTIVIRUS 122
3.14 CONTROLLO DEL SOFTWARE.....124
3.15 RISERVATEZZA E AUTENTICITA' DEI DATI.....124
3.16 AUTENTICAZIONE 125
3.17 SICUREZZA ORGANIZZATIVA.....126

DATABASE, LE RETI E LA MULTIMEDIALITÀ

1 Database e reti LAN

1.1 I calcolatori

L'utilizzo sempre più diffuso del computer ha numerose conseguenze dirette ed immediate sulla vita lavorativa delle persone: possibilità di comunicare vie rete, scrivere utilizzando i *word processor*, possibilità di utilizzare reti interne alle aziende, sono solo la punta di un iceberg che si fa di giorno in giorno sempre più grande.

Oggi chiunque è in grado di utilizzare un PC per elaborare e gestire informazioni e utilizzarle per lavoro o per altri scopi.

Ma qual è il vero valore dei computer? Quali sono le loro potenzialità?

La loro principale caratteristica è la capacità di elaborare grandi quantità di dati in poco tempo. questo fatto consente di effettuare calcoli o elaborare informazioni in un tempo molto ridotto.

La velocità di calcolo di un computer e la sua conseguente capacità di elaborare informazioni rappresentano un enorme vantaggio nel mondo di oggi, caratterizzato dalla presenza di una grande massa di informazioni che hanno bisogno di essere elaborate e gestite.

La velocità di calcolo è determinata dalla CPU (*central processor unit*)

L'unità centrale di elaborazione, è anche chiamata, esclusivamente nella sua implementazione fisica, processore, ed è uno dei due componenti principali del PC. Compito della CPU è quello di leggere i dati dalla memoria ed eseguirne le istruzioni. La CPU decifra ed esegue le istruzioni che risiedono nella memoria principale grazie a due unità che si chiamano:

- **CU** o unità di controllo (Control Unit);
- **ALU** o unità aritmetico logica (Arithmetic Logic Unit).

Vediamo di esaminare più in dettaglio le funzioni di queste due componenti della CPU.

La **CU** è quella parte di CPU che controlla e organizza l'attività dei dispositivi collegati all'elaboratore: recupera tutte le istruzioni dalla memoria, le decifra e le esegue.

La **ALU** è l'unità aritmetico logica in cui vengono effettuati i calcoli aritmetici e logici richiesti dalle istruzioni del programma.

La **RAM** (Random Access Memory) è invece una memoria volatile: il suo contenuto viene perso in caso di spegnimento del computer. Contiene i dati e le istruzioni dei programmi in esecuzione. Maggiore è la quantità di memoria RAM installata migliori saranno le prestazioni del PC.

La crescente diffusione dei computer e l'aumento costante della velocità e della capacità di calcolo dei PC consentono proprio l'aumento generalizzato e diffuso della capacità di elaborazione.

Tipologie di computer

Il primo calcolatore elettronico fu **l'ENIAC**, (Electronical Numerical Integrator And Calculator) che nacque nei primi anni '40 e venne utilizzato fino al 1955. Era costituito da 18.000 valvole ed aveva una dimensione di circa 160 mq.

L'evoluzione tecnologia costante ci permette di avere a disposizione diversi tipi di computer che variano in potenza e dimensioni.

Mainframe: è un grande elaboratore centrale, con ottime prestazioni in termini di capacità di calcolo e di memoria. Abitualmente viene utilizzato per gestire medie e grandi imprese. Un mainframe può servire contemporaneamente un elevato numero di utenti.

Mini Computer: è un calcolatore molto simile al *mainframe* da cui si differenzia per il formato e la potenza. Un Mini Computer, infatti, può servire contemporaneamente non più di 200 utenti.

Personal Computer: sono piccoli elaboratori ideati per l'uso personale. Il termine PC fu coniato la prima volta dall'IBM per identificare il loro primo microcomputer. L'uso più significativo del computer è in ambito lavorativo. In ambito familiare, invece, è prevalso da sempre l'uso ricreativo, anche se da qualche tempo si sta diffondendo sempre più il telelavoro. Il PC, ormai, si è affermato su scala mondiale: milioni di persone possiedono macchine in grado di 9 elaborare dati e documenti e creare immagini. Col tempo, i prezzi si sono notevolmente ridotti: in media, variano da alcune centinaia di euro ad oltre cinquemila euro.

Laptop computer: (chiamato anche notebook computer o più comunemente portatile) è un PC di piccole dimensioni, adatto al trasporto e caratterizzato da alimentazione a batteria (ricaricabile), schermo piatto a cristalli liquidi, dimensioni ridotte. Il costo di un portatile è circa il doppio rispetto a un normale PC di potenza equivalente. Un computer portatile offre notevoli vantaggi ma comporta anche diversi inconvenienti. È leggero e maneggevole,

funziona per qualche ora senza la necessità di un'alimentazione a corrente e si può portare con estrema facilità in viaggio o in vacanza. Per quanto riguarda gli svantaggi, il laptop è più caro di un normale PC, ha una limitata capacità di aggiornamento ed espansione e non dà la possibilità di collegarsi a molte periferiche.

Il più piccolo dei computer è il **Palmare**, computer tascabile con potenzialità e prestazioni limitate.

Network computer: computer a basso costo, che funziona grazie ad un server a cui è collegato e dal quale preleva le risorse necessarie per poi elaborarle in locale.

Workstation: è un sistema con elevate prestazioni di calcolo e funzioni grafiche, solitamente utilizzato per la progettazione.

Tra i tipi di computer includiamo, inoltre, i **Super computer**, sistemi dotati di una elevata potenza elaborativa e che svolgono funzioni di calcolo molto complesse.

Terminale: è la postazione di lavoro che utilizza la rete per stabilire una connessione a sistemi di elaborazione remoti per l'accesso a dati e servizi.

Esistono due tipi di terminali:

- **terminale "intelligente":** dotato di micro-processore e di memoria ed in grado, quindi, di elaborare informazioni in maniera autonoma anche in assenza di collegamento telematico con il computer centrale.
- **terminale "stupido":** non possiede né microprocessore, né memoria e quindi non può elaborare dati ma semplicemente leggerli dal computer centrale e chiederne l'elaborazione allo stesso.

Troviamo inoltre i **terminali self-service**, come gli sportelli automatici, gli sportelli informativi o le biglietterie automatiche che hanno uno schermo sensibile al tatto, pochi tasti, una guida in linea ed un uso diffuso di menu.

1.2 Hardware e Software

La prima scomposizione di un calcolatore e` relativa ai seguenti macro-componenti

- **Hardware**: Insieme delle sue componenti elettroniche e meccaniche
- **Software**: Insieme dei programmi che consentono all'hardware di svolgere dei compiti utili. Il software si divide in *software di base* (tra cui il sistema operativo) e il *software applicativo.*

In informatica il **sistema operativo** (abbreviato spesso nel suo acronimo SO, o all'inglese OS, *operating system*) è l'insieme di routine e strutture dati responsabile del controllo e della gestione dei componenti hardware che costituiscono un computer e dei programmi che su di esso vengono eseguiti. Il sistema operativo mette anche a disposizione dell'utente una interfaccia software (grafica o testuale) per accedere alle risorse hardware (dischi, memoria, I/O in generale) del sistema. Il compito principale del sistema operativo è quello di permettere all'utente, umano o non, di interagire direttamente con la macchina.

Tra i sistemi operativi maggiormante conosciuti oltre a MS Windows troviamo **Linux** e **Apple Mac OS**.

Linux (o **GNU/Linux**) è un sistema operativo libero di tipo Unix Molto conosciuto nell'uso server, è usato come sistema operativo su una gran varietà di hardware; dai computer desktop ai supercomputer, fino a sistemi embedded come cellulari e palmari, e ai netbook.

Mac OS X è il sistema operativo sviluppato da **Apple Inc**. per i computer Macintosh, nato nel 2001 per combinare le note caratteristiche dell'interfaccia utente del Mac OS originale con la stabilità e le prestazioni di un potente sistema operativo di derivazione Unix.

Particolare rilievo assumono, nell'ambito del software applicativo, i software di produttività personale ovvero applicazioni che permettono ad un utente di un computer di creare dei contenuti quali documenti di testo, presentazioni o grafici. Le categorie più note sono gli elaboratori di testo e i fogli elettronici, ma rientrano in questo tipo di software anche i programmi che permettono di creare

presentazioni, volantini e brochure, siti internet, database ecc. In alcuni casi le funzionalità di questi software sono ridotte rispetto a quelle di software orientati ad un uso più professionale o specialistico.

Spesso un unico produttore commercializza più categorie di software di produttività personale e li raccoglie in *Suite* (MS® Office, Open Office, Star Ofice ecc).

1.3 Files

E' pressoché impensabile poter pensare di lavorare con il PC senza conoscere le principali tipologie di *files* in uso e le principali differenze non solo rispetto al tipo ma anche rispetto alle funzionalità.

Un **file** (termine inglese per "archivio") è un contenitore di informazione digitalizzata. Le informazioni codificate al suo interno sono leggibili solo da software. Il contenuto dei file è normalmente conforme ad un particolare **formato**, e per ciascun formato esistono una o più applicazioni che sono in grado di interpretarne e/o di modificarne il contenuto ("aprire" il file).

In considerazione dei molteplici software di produttività personale presenti sul mercato – liberi e non – e delle diverse tipologie di sistema operativo in uso si è rivelato sempre più necessario orientarsi verso formati di file universali e interscambiabili ovvero "leggibili" da qualunque programma con qualunque sistema operativo.

Nell'ambito della videoscrittura questo formato è il **formato RTF**

.RTF

L' RTF è un formato di interscambio dati creato in origine per facilitare lo scambio tra versioni diverse di Word e tra il mondo Windows e Mac.

È un formato "portabile" per la definizione di documenti comprendenti formattazione di paragrafo, di carattere e di pagina. Ogni documento Microsoft Word può essere salvato in formato RTF. Viceversa Microsoft Word, e così anche tutti i principali tool per la videoscrittura, può caricare un file in formato RTF. Queste le caratteristiche salienti:

- RTF mantiene (in parte) la formattazione del file originale.
- È un file di tipo testo.
- È uno standard "de facto", non "de iure" (esistono varie versioni, non sempre mutuamente compatibili)
- Lascia la possibilità di modificare il file sorgente.
- Generalmente non trasmette macro virus e per questo motivo il formato RTF torna utile nello scambio di documenti per e-mail.

Per garantire la massima portabilità di un documento sarebbe utile salvare sempre il file in formato .RTF

.PDF

Il **Portable Document Format**, comunemente abbreviato **PDF**, è un formato di file basato su un linguaggio di descrizione di pagina sviluppato da Adobe Systems nel 1993 per rappresentare documenti in modo indipendente dall'hardware e dal software utilizzati per generarli o per visualizzarli.

Un file PDF può descrivere documenti che contengono testo e/o immagini in qualsiasi risoluzione.

.ZIP

Quando parliamo di file .ZIP o .RAR (vedi dopo) parliamo di files compressi.

Un file **ZIP** è un file conformato di compressione dei dati molto diffuso.

.RAR

Quando parliamo di file .RAR o .ZIP (vedi sopra) parliamo di files compressi.

RAR è un formato di file proprietario per l'archiviazione e la compressione di dati, sviluppato da Eugene Roshal. RAR è infatti un acronimo di ***R****oshal* ***AR****chive*.

MS Office / Open Office.org

Negli ultimi anni si è sempre più diffuso il software open source di cui abbiamo già detto. Per quanto concerne le *suite* di produttività personale occorre avere presente la tabella di raffronto qui riportata:

	MS Office	OpenOffice
Videoscrittura	.doc / .docx	.sxw / .odf (.odt)
Calcolo	.xls / .xlsx	.sxc / .odf (.ods)
Presentazioni	.ppt / .pptx	.sxi / .odf (.odp)
Database	.mdb	.odf (.odb)

Il formato XML

XML (acronimo di **eXtensible Markup Language**) è un metalinguaggio di markup, ovvero un linguaggio marcatore (**tag**). Permette di definire in modo semplice nuovi linguaggi di markup da usare in ambito Web. Il nome indica quindi che si tratta di un linguaggio marcatore (*markup language*) *estensibile* (*eXtensible*) in quanto permette di creare **tag** personalizzati.

Il linguaggio XML è inoltre indipendente dalla piattaforma, ossia qualsiasi applicazione progettata per utilizzarlo consente di leggere ed elaborare dati XML, indipendentemente dall'hardware o dal sistema operativo.

1.4 Gestire le informazioni

Gestire le informazioni

La possibilità di utilizzare strumenti informatici consente di gestire informazioni di ogni tipo

Ogni ufficio e ogni struttura lavorativa usa archivi, grandi o piccoli contenenti dati necessari al proprio lavoro (clienti, codici, fatture, ecc…).

Il problema che si presenta a chiunque abbia a che fare con i dati è:

COME FARE A GESTIRLI?

È possibile progettare l'archivio in modo che sia facilmente consultabile, che le informazioni siano facilmente rintracciabili, che l'archivio stesso sia facilmente modificabile? In altre parole che sia veramente utile al lavoro che si sta svolgendo?

L'INFORMATICA RAPPRESENTA UN GRANDE AIUTO E OFFRE POTENZIALITA' DI GESTIONE DEI DATI DI GRANDE EFFICACIA.

La difficoltà a ottenere una facile consultazione dei dati e delle informazioni necessarie all'attività lavorativa è uno dei problemi principali con cui devono continuamente "combattere" le aziende o gli uffici. È stato calcolato che ogni anno un enorme numero di ore lavorative va perduto per archiviazione non corretta o non efficiente dei dati.

1.5 DAI FASCICOLI AI DATABASE

Un database può essere considerato come un insieme di informazioni collegate ad un oggetto o ad uno scopo particolare. I database sono enormi raccoglitori d'informazioni che conservano in ***formato digitale***: essi contengono non solo documenti di testo ma anche suoni, video, immagini ecc.. cioè tutto ciò che la tecnologia è in grado di trasformare in formato digitale

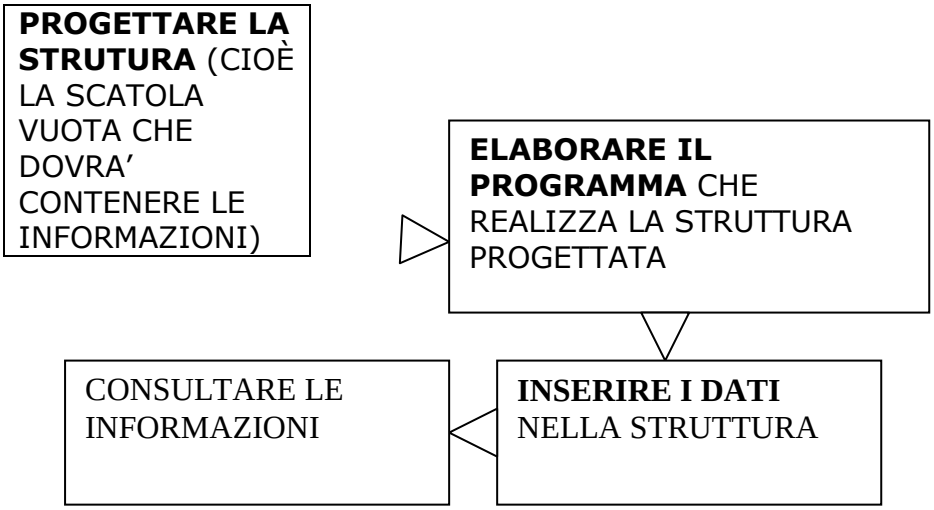
Oltre a immagazzinare informazioni di diverso tipo, i database consentono anche la loro elaborazione e riorganizzazione logica in modo da **soddisfare le esigenze di consultazione** e/o di risoluzione di uno specifico problema. In questo modo consentono anche di individuare le informazioni utili e di evidenziare collegamenti trasversali tra i dati stessi.

Non sono un semplice archivio, ma un vero e proprio programma di gestione delle informazioni.

1.6 REALIZZAZIONE DI UN DATABASE

COME SI FA A REALIZZARE E A FAR FUNZIONARE UN DATABASE?

La realizzazione di un database comporta una serie di passaggi logico-operativi che iniziano con la sua progettazione e terminano con la realizzazione della struttura.



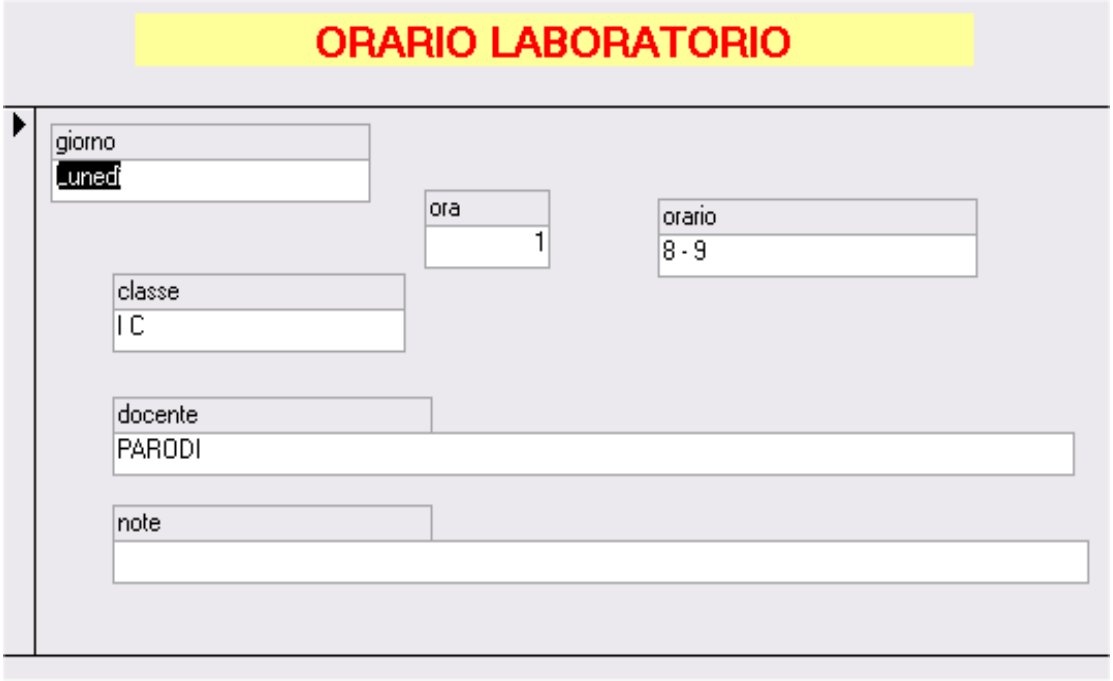
PER REALIZZARE UN DATABASE (in estrema sintesi)

Le attività di inserimento e consultazione delle informazioni di solito vengono svolte dagli utenti finali ai quali viene consegnato il database vuoto riempito successivamente di dati e informazioni. La creazione del database è infatti un'attività di programmazione e viene di solito eseguita da esperti.

Esistono oggi sul mercato facili programmi specializzati nella creazione di database che consentono di creare il proprio database in maniera relativamente semplice. Uno dei più famosi è il software Access della Microsoft.

1.7 INSERIMENTO DATI

In genere le operazioni di inserimento e visualizzazione dei dati vengono effettuate attraverso *maschere* nelle quali sono visualizzati i campi specifici per le informazioni. Le maschere hanno il compito di visualizzare i campi e far comprendere che tipo di dato deve essere inserito.

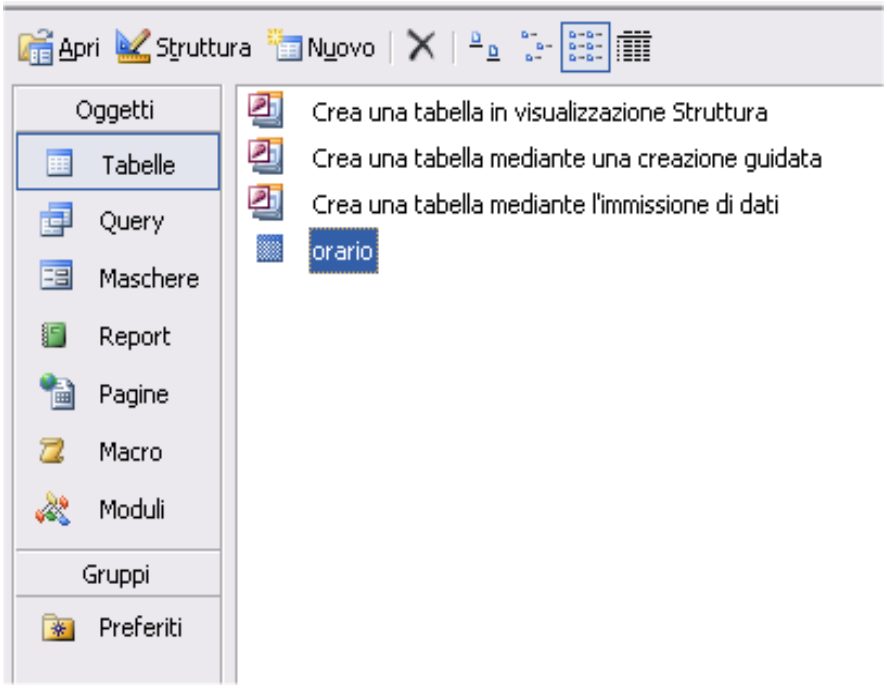


Le maschere rappresentano l'elemento del database che viene a contatto con l'utilizzatore e devono essere di facile comprensione e utilizzo. Vengono chiamate anche interfacce del database perché attraverso di esse viene aggiornato e consultato.

1.8 ELEMENTI DI UN DATABASE

GLI ELEMENTI FONDAMENTALI DI UN DATABASE SONO:

Tabelle Strutture del database che contengono i dati	**Report** Schemi predefiniti che servono alla stampa dei dati. Hanno una struttura visiva dei dati già predefinita in relazione alle esigenze degli utenti.
Query o interrogazioni Sono strumenti che consentono di visualizzare solo una determinata categoria di dati.	**Maschere** Interfacce di visualizzazione delle informazioni



Particolare importanza rivestono le tabelle; le informazioni nel DB infatti non sono casuali ma vengono raggruppate in strutture che contengono dati simili o appartenenti ad una stessa categoria: le tabelle.

Il DATABASE non è altro che un insieme di tabelle ciascuna costituita da un insieme di dati che rappresenta una categoria dell'archivio.

LA TABELLA RAPPRESENTA DUNQUE UN INSIEME DI DATI OMOGENEI TRA LORO.

I database relazionali consentono di associare i dati di una tabella con quelli di un'altra attraverso i valori corrispondenti delle tabelle. In questo modo è possibile inserire le informazioni una volta sola e rendere il database più efficiente

SQL

SQL (*Structured Query Language*) è un linguaggio creato per l'accesso a informazioni memorizzate nei database. Alla base di tutte le query, dunque di tutte le interrogazioni di una base di dati, di norma cè il linguaggio SQL o qualche sua diretta derivazione (MS® SQL, MySQL ecc,)

1.9 RECORD e CAMPI

Viene indicato con il termine "Campo" un'area destinata allo stesso tipo di dati da inserirsi in una tabella. Il tipo di dato, relativo alla struttura di una tabella, e quindi il Campo, può essere di tipo:

- Contatore
- Numerico
- Testo
- Logico
- Memo
- Altro.

I campi possono essere a lunghezza fissa oppure variabile, dipende da tipo di accesso che si avrà per quel dato archivio.

Il "Record" è un insieme di campi che sono in relazione tra di loro. In relazione tra di loro, significa che quello che è espresso in un determinato campo di un record è esclusivamente riferito (e quindi, è in relazione) agli altri campi dello stesso record.

1.10 PROGETTARE UN DATABASE

Quali sono i passi necessari alla creazione di un DB?

1. IDENTIFICARE CON CHIAREZZA I DATI DA INSERIRE NEL DATABASE, LA TIPOLOGIA DELLE INFORMAZIONI E LE OCCASIONI DI CONSULTAZIONE
2. CREARE LE TABELLE NECESSARIE (no alle ridondanze e mantenere la consistenza)
3. PROGETTARE I CAMPI
4. DEFINIRE LE RELAZIONI TRA LE TABELLE
5. IMPLEMENTAZIONE

SE UN DB PRESENTA UNA NON EFFICIENTE ORGANIZZAZIONE DELLE TABELLE SI DICE CHE NON È NORMALIZZATO.

1. Attenzione alla corretta definizione delle informazioni. Ogni modifica successiva potrebbe essere molto onerosa
2. Le tabelle sono costituite di solito da righe (record) che rappresentano una scheda. Ogni scheda contiene più campi di informazioni. La progettazione delle tabelle è un'operazione di grande difficoltà che deve essere compiuta tenendo a mente alcuni criteri generali, i primi dei quali sono:

- Evitare le ridondanze (inserire un dato una sola volta in una tabella e non ripetere l'operazione più volte)
- Mantenere la consistenza dei dati (Ogni tabella deve contenere informazioni omogenee tra loro, legate allo stesso argomento)

3. I campi corrispondono alle colonne della tabella. L'operazione di realizzazione consiste in pratica nella costruzione dei campi cioè nell'inserimento delle informazioni in ciascuna tabella. Utilizzare sempre dati puri (non derivanti da funzioni) e individuare i campi che rappresentano il collegamento tra diverse tabelle (chiave primaria);
4. <u>I collegamenti tra le tabelle (o meglio tra le informazioni contenute nelle tabelle) vengono realizzati mediante i campi di collegamento (chiavi primarie) e altre chiavi esterne</u>. Si tratta cioè di individuare che tipo di collegamento esiste tra i dati delle tabelle. Come esempio analizziamo un DB costituito da due tabelle:
    a) tabella che contiene i dati anagrafici di dei fornitori di un'azienda
    b) tabella che contiene le fatture emesse. In questo caso la relazione in questione è di tipo uno a molti perché ciascun fornitore potrà emettere molte fatture. Si tratta cioè di creare un collegamento tra un campo della tabella a (fornitore) e una serie di campi della tabella b (fatture emesse).

1.11 RETI LAN

Oggi le reti aziendali LAN (Local Area Network) sono sempre più diffuse anche se poco comprese e conosciute.

Quali sono gli elementi che costituiscono una rete locale?

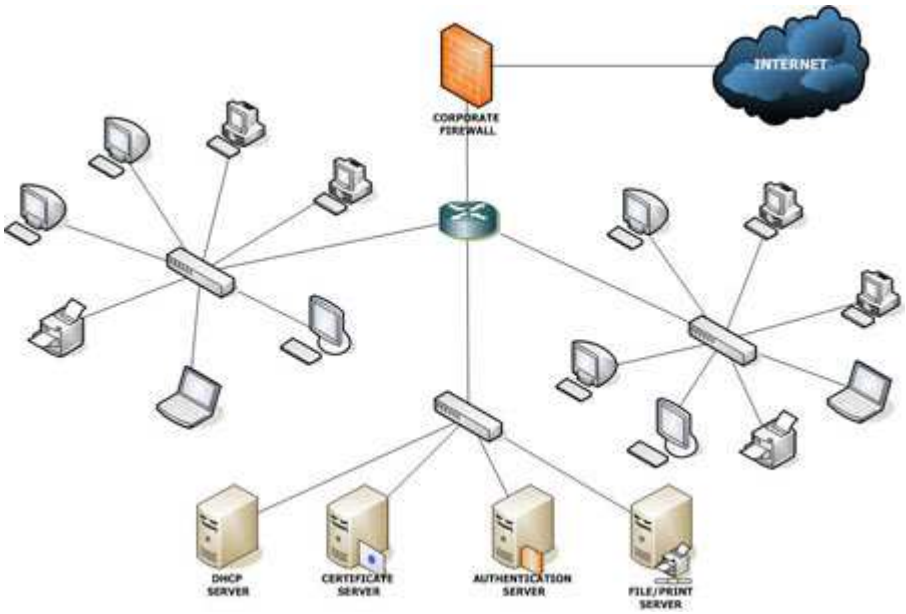
Una rete è costituita da una serie di computer collegati tra loro in grado di scambiare dati e comunicare tra loro.

Gli elementi di base di una rete locale sono:

SERVER: computer che ospita risorse e strumenti condivisi dagli altri. È il cervello della rete.

CLIENT: computer che accede alle risorse presenti nel server.

ACCESSORI: dispositivi diversi (stampanti, hard disk esterni, ecc).



Naturalmente questi sono solo gli elementi di base di una rete LAN che in realtà è quasi sempre più complessa ed articolata. Ad esempio con una rete LAN e' possibile accedere anche ad altre risorse come ad esempio CD-ROM ma queste vengono considerate risorse secondarie perché connesse non direttamente alla rete.

WAN e MAN

Con i termini WAN e MAN sono indicate due tipologie di reti maggiormente complesse:

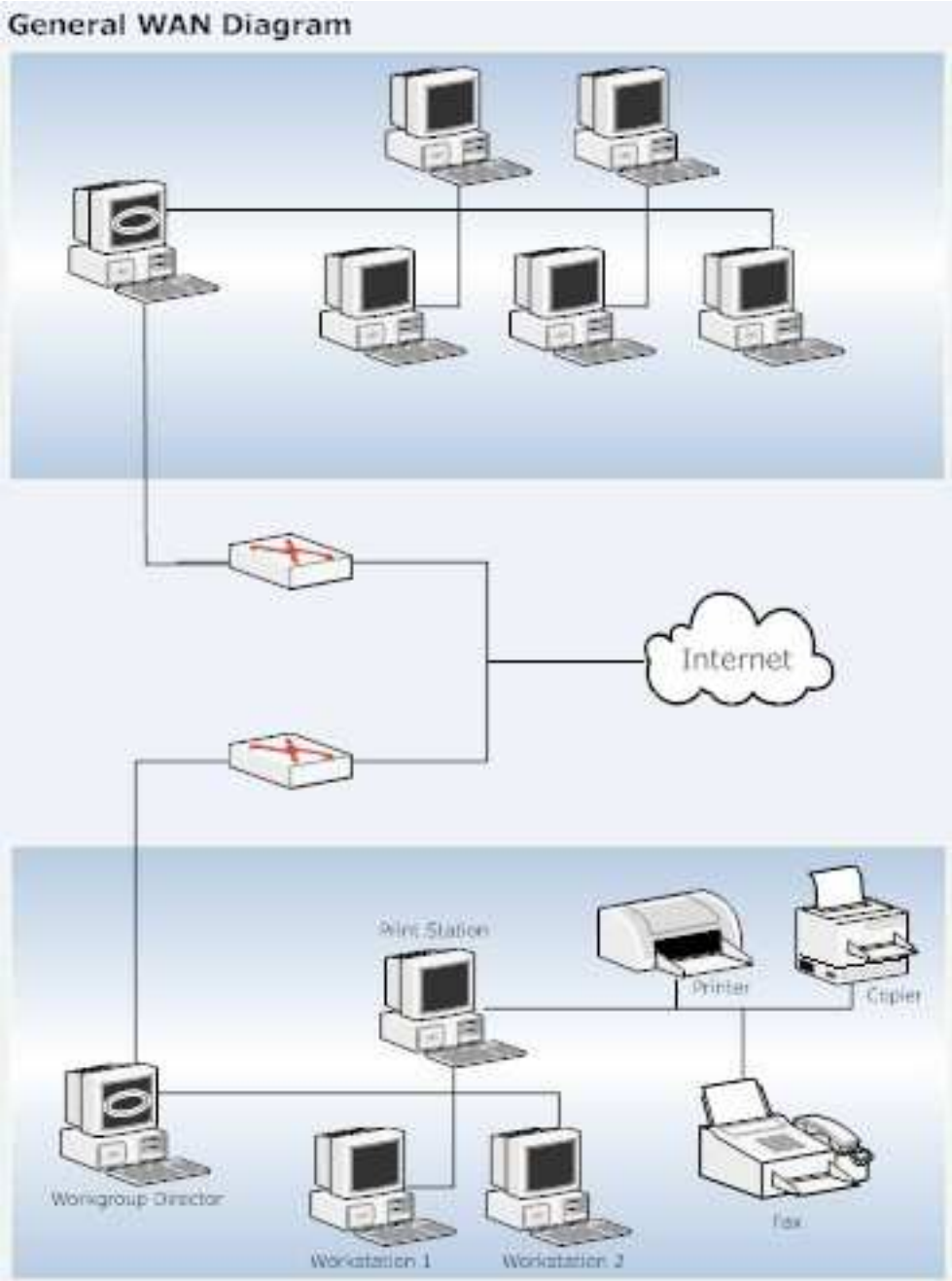
Una rete WAN è una rete che si estende coprendo zone dall'ambito fino all'intero globo. Come mezzo di comunicazione si utilizza la rete telefonica in quanto era già esistente e garantiva la copertura dell'intero globo, senza bisogno di nessun intervento di cablaggio.

Una rete MAN Una rete metropolitana o (in inglese metropolitan area network, abbreviato in MAN) è una rete telematica che di solito ricopre un'intera città.

Storicamente le MAN sono nate per fornire servizi di tv via cavo alle città dove c'era una cattiva ricezione terrestre. In pratica un'antenna posta su una posizione favorevole, distribuiva poi il segnale alle case mediante cavo.

Prima la cosa è avvenuta a livello locale, successivamente si sono create grosse aziende che hanno richiesto di cablare intere città, soprattutto negli Stati Uniti. Quando il fenomeno Internet è esploso, queste società hanno ben pensato di diffondere la comunicazione internet anche attraverso il cavo TV utilizzando la stuttura preesistente.

Tipicamente questa struttura usa fibra ottica per collegamento.



1.12 SERVER

La parola Server viene utilizzata di solito per descrivere in termini generici un computer multiutente cioè un computer che funziona per numerosi utenti differenti.

In realtà esistono numerose "tipologie" di server ciascuno specializzato in base alla funzione che svolge.

Uno dei più comuni è il server di file, meccanismo centralizzato che **contiene tutti i file utilizzati da un gruppo di utenti che per lavorare "pescano" nel server.**

In questo modo i file sono in posizione centralizzata e non dispersi in numerose macchine client.

Questa struttura fornisce numerosi vantaggi tra i quali una grande facilità di individuazione del file, facilità di gestione degli identificativi di accesso (nel caso siano necessari) migliore protezione dei dati, facilità nell'effettuare le operazioni di back-up, maggiore velocità (rispetto a file che si trovano in altre macchine ma non in un server)

Altri tipi di server di solito utilizzati sono server di stampa e **server di applicazioni, nei quali il server ospita solo programmi da eseguire**. Uno dei principali vantaggi è che il prezzo per acquistare e mantenere un programma multiutente e' di solito sensibilmente inferiore a quella che si avrebbe acquistando numerose applicazioni separate.

Proprio per questo motivo è importante fare attenzione ad installare in un server un programma acquistato per uso individuale potrebbe violare le condizioni della licenza acquistata. Per poter fare questa operazione e' necessario che il pacchetto sia multiutente.

1.13 TIPOLOGIA DI RETI

I PRINCIPALI TIPI DI RETE SONO DUE:

RETE PARITETICA

Nelle reti paritetiche ciascun dispositivo **può essere contemporaneamente client o server**. Tutti sono in grado di accedere direttamente ai dati al software e alle altre risorse.

RETE BASATA SUL SERVER

Nelle reti basate su server **ogni computer comunica con il server** che rappresenta il cervello e la centrale operativa della rete.

Reti paritetiche

Vantaggi

Sono facili da usare e da realizzare (in realtà sono costituite da una serie di computer client con un sistema operativo di rete che consente una condivisione delle risorse); sono poco costose perché non hanno server specifici di solito più costosi e sofisticati; possono essere costruite mediante programmi noti e facili da usare; sono in genere più resistenti agli errori.

Svantaggi

Non sono sicure (ciascun utente deve gestire una parola d'ordine e provvedere alla sicurezza individualmente); è più difficile il ritrovamento e la gestione dei file; ciascun utente deve reperire le risorse che sono necessarie nella rete; il backup dei dati avviene di solito senza coordinamento perché ciascun utente ha la responsabilità della propria macchina.

OGNI MACCHINA DELLE RETI PARITETICHE E' CONFIGURATA PER ESSERE ALLO STESSO TEMPO CLIENT O COMPUTER INDIVIDUALE E, SE DEVE LAVORARE IN GRUPPO, LA SUA EFFICENZA POTREBBE DIMINUIRE

DI SOLITO QUESTO TIPO DI RETE COSTITUISCE LA SCELTA PRIVILEGIATA DI PICCOLE STRUTTURE CHE HANNO PICCOLI BUDGET

Reti basate su server

In questo tipo di rete i computer non devono interfacciarsi con altri computer analoghi; di solito sono più efficienti e sicure in quanto la sicurezza e' gestita centralmente e non lascia buchi causati dall'anello più debole della catena come avviene invece in quelle paritetiche; le operazioni di back-up sono molto più efficaci in quanto gestiti centralmente; in genere si verificano miglioramenti delle prestazioni per i computer legati alle reti, a causa dell'ottimizzazione della configurazione del server e del fatto che ciascun client si interfaccia direttamente con il server.

Svantaggi

La rete basata su server di solito costa molto di più (software e hardware); i costi operativi sono maggiori di solito (e' necessario un responsabile esperto per la manutenzione); se si rompe il server si blocca la rete.

2 Internet e la Multimedialità

2.1 INTERNET

Internet, *the net*, la rete delle reti. Una ragnatela, una rete informatica, anzi una serie di reti di calcolatori connesse tra loro.

Costituita da alcune centinaia di milioni di computer collegati tra loro con i più svariati mezzi trasmissivi, Internet è anche la più grande rete di computer attualmente esistente e mai esistita, in ragione di ciò è infatti definita "la rete delle reti" o "la rete globale". In quanto rete di telecomunicazioni (una rete di computer è una tipologia di rete di telecomunicazioni) è invece seconda alla rete telefonica pubblica, anch'essa rete di telecomunicazioni mondiale ma coprente il pianeta in modo più capillare di Internet, motivo per cui inizialmente è stata largamente utilizzata per accedere a Internet dagli utenti comuni (singoli e aziende), e tutt'oggi lo è ancora, anche se, in un futuro non troppo lontano, con il miglioramento della tecnologia **VoIP** (VOICE OVER INTERNET PROTOCOL), è destinata a scomparire sostituita/inglobata da Internet in quanto basata su una tecnologia, la commutazione di pacchetto, comportante maggiore efficienza delle infrastrutture di rete. (*Wikipedia*)

Una rete di calcolatori è dunque un sistema che permette la condivisione di informazioni e risorse (sia hardware che software) tra diversi calcolatori. Il sistema fornisce un servizio di trasferimento di informazioni ad una popolazione di utenti distribuiti su un'area più o meno ampia.

La caratteristica predominante di Internet è la sua struttura a ragnatela che consente ai dati di percorrere strade multiple e alternative.

INTERNET È IN GRADO DI COLLEGARE COMPUTER IN TUTTI I POSTI DEL MONDO.

Internet consente di percorrere strade multiple, contemporanee e alternative.

In pratica vuol dire che i dati e le informazioni non passano sempre attraverso una strada definita ma viaggiano nella rete fino ad arrivare alla destinazione voluta. Può anche accadere che per inviare i dati da Roma a Firenze questi transitino per New York. Sempre ad alta velocità.

Uno degli aspetti più interessanti della rete è proprio questa sua "casualità" e capacità di far comunque passare le informazioni. I dati vengono infatti scomposti alla partenza in pacchetti, opportunamente codificati e "marchiati" e inviati. Ciascun pacchetto è in grado di viaggiare autonomamente anche per strade differenti per poi ricomporsi all'arrivo.

2.2 www, mail, ftp e gli altri protocolli d Internet

La comunicazione su Internet non è solo www ovvero il limitarsi a s*fogliare* le pagine web; esistono in realtà molte *applicazioni* che sfruttando opportuni *protocolli* permettono di inviare e ricevere posta elettronica, di trasferire file anche di grandi dimensioni, di telefonare, di video chiamare (e ricevere

telefonate video) e altro ancora. E' opportuno conoscere i protocolli base e le più note *porte di comunicazione* utilizzate, meglio conosciute come *Well Know Port*

Servizi (Applicazioni) con *well-know port number*:

- Porta 21 – *ftp* – File Transfer Protocol
- Porta 22 – *ssh* – Secure Shell
- Porta 25 – *smtp* – Simple Mail Transfer Protocol
- Porta 80 – *http* – World Wide Web
- Porta 110 – *pop3* – Post Office Protocol.

Ad esempio Il protocollo HTTP (Hyper Text Transfer Protocol) viene usato da tutti i client e server web e gestisce il modo con cui questi si scambiano pagine HTML o altri file.

Il protocollo http utilizza la porta 80 del calcolatore. Scrivere l'indirizzo web http://www.unige.it e http://www.unige.it:80 è la stessa cosa

Il client web (cioè un browser come Microsoft Internet Explorer, Netscape Navigator, Opera ecc.) utilizza l'HTTP per richiedere file al server web. In primo luogo vengono richieste pagine HTML, che dopo essere state ricevute, vengono processate dal browser che provvede a fare richiesta di eventuali nuovi file richiamati nel codice HTML (immagini, fogli di stile css, script esterni ecc.) e a visualizzare il tutto sul monitor dell'utente.

2.3 VoIP

TELEFONARE CON INTERNET

Voice over IP (*Voce tramite protocollo Internet*), acronimo VoIP, è una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata che utilizza il protocollo IP. Grazie a numerosi provider VoIP è possibile effettuare telefonate anche verso la rete telefonica tradizionale (PSTN). Il vantaggio principale di questa tecnologia sta nel fatto che essa elimina l'obbligo di riservare della banda per ogni telefonata (communtazione di circuito), sfruttando l'allocazione dinamica delle risorse, caratteristica dei protocolli IP (commutazione di pacchetto). Vengono instradati sulla rete pacchetti di dati contenenti le informazioni vocali, codificati in forma digitale, e ciò solo nel momento in cui è necessario, cioè quando uno degli utenti collegati sta parlando.

Fra gli altri vantaggi rispetto alla telefonia tradizionale si annoverano:

- minore costo per chiamata, specialmente su lunghe distanze;
- minori costi delle infrastrutture: quando si è resa disponibile una rete IP nessun'altra infrastruttura è richiesta;
- nuove funzionalità avanzate;
- l'implementazione di future opzioni non richiederà la sostituzione dell'hardware.

Le conversazioni VoIP non devono necessariamente viaggiare su Internet, ma possono anche usare come mezzo trasmissivo una qualsiasi rete privata basata sul protocollo IP, per esempio una LAN all'interno di un edificio o di un gruppo di edifici. I protocolli usati per codificare e trasmettere le conversazioni VoIP sono solitamente denominati *Voice over IP protocols*.

2.4 BREVE STORIA DI INTERNET

Primi anni ’60	viene creato in USA un gruppo di lavoro nella Difesa Americana con l’obiettivo di creare una rete di collegamento sicura.
1969	nasce Arpanet la prima rete di calcolatori basata sui principi di Internet (assenza di direttrici preferenziali, possibilità per i dati di muoversi secondo una qualsiasi linea di collegamento per poi ricombinarsi alla fine).
Anni ’70 e ’80	nascono, si sviluppano e si collegano reti locali, nazionali ed internazionali (soprattutto nel mondo scientifico) che utilizzano la logica di Internet. Si afferma un protocollo di comunicazione comune per Internet (sistema di codificazione dei dati che viaggiano nella rete) il TCP/IP.
Primi anni ’90	nasce il World Wide Web che consente la fruizione ‘di massa’ di Internet. È possibile fruire su Internet immagini, video, audio, testi, ecc…

1. In risposta all’invio del primo invio di un astronauta sovietico nello spazio l’Amministrazione statunitense creò l'Advanced Research Projects Agency (ARPA), una struttura interna al Dipartimento della Difesa, che aveva lo scopo di ristabilire il primato americano nelle scienze applicate al settore militare. Il problema principale che tali scienziati si trovarono ad affrontare era quello di proteggere le comunicazioni tra i centri di comando in caso di attacco nucleare e la loro risposta fu quella di creare una rete "anarchica" priva cioè di qualsiasi autorità centrale e in grado di trasmettere dati anche se la maggior parte dei suoi collegamenti fosse stata interrotta. Internet è anarchica perché è stata progettata in questo modo. Tutti nodi dovevano essere indipendenti: i messaggi sarebbero stati scomposti in pacchetti (opportunamente codificati) e inviati separatamente. Ciascuno avrebbe potuto seguire strade differenti e solo alla fine sarebbero stati ricomposti per costituire il messaggio iniziale. Se per qualsiasi motivo si fosse verificato un blocco, il pacchetto sarebbe stato immediatamente re-indirizzato per una strada differente. Il

sistema così pensato è più inefficiente rispetto ad una linea telefonica ma sicuramente è molto più sicuro.

2. Nel 1969 nasce la prima rete con questi principi chiamata ARPANET. Con l'evoluzione delle tecnologie informatiche le reti locali crescono in maniera continua e progressiva e viene definito un sistema comune di classificazione e codificazione dei dati chiamato protocollo TCP/IP.
3. Negli anni seguenti si sviluppano reti nazionali e internazionali e si creano dorsali costituite da supercalcolatori che contribuiscono al diffondersi dell'utilizzo di queste tecnologie.
4. Tuttavia la vera e propria esplosione di Internet si ha con la nascita del WWW, un sistema di visualizzazione e di accesso semplice e di facile comprensione.

Il Web è stato lo strumento che ha "liberalizzato" l'accesso alla rete stessa perché ha semplificato la navigazione e la ha resa accessibile a tutti.

2.5 WORLD WIDE WEB

Il www nasce ad opera di Tim Berners-Lee al CERN di Ginevra.

Berners-Lee ha coniato il nome di *World Wide Web*, ha scritto il primo server per il World Wide Web, *<u>httpd</u>* e il primo programma client (un browser e un editor), *<u>WorldWideWeb</u>*, nell'ottobre del 1990. Ha scritto inoltre la prima versione del linguaggio di formattazione di documenti con capacità di collegamenti ipertestuali conosciuto come HTML.

Le sue specifiche iniziali per URL, HTTP e HTML sono state in seguito perfezionate e discusse da una vasta comunità di utenti e programmatori, dando vita al fenomeno Internet.

Due definizioni importanti:

- url - Un **Uniform Resource Locator** o URL è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o un'immagine.
- http - **L'Hyper Text Transfer Protocol** (HTTP) (protocollo di trasferimento di un ipertesto). Usato come principale sistema per la trasmissione di informazioni sul web.

Internet deve la sua fortuna proprio alla modalità di accesso **<u>www</u>**: non esistono comandi e la fruizione dei dati avviene con un sistema ad oggetti. In questo modo non è necessario conoscere e digitare codici o linguaggi particolari ma semplicemente usare il mouse e "cliccare" sull'oggetto di interesse. Con il <u>www</u> chiunque è in grado ricreare il proprio sito Internet e mettere a disposizione informazioni personalizzate.

In ambiente WEB, con appositi programmi di navigazione, i browser (Mosaic, Netscape, Microsoft Explorer), è possibile spostarsi da un sito all'altro e da un documento all'altro con il semplice clic del mouse sulle parole sottolineate (links). Questo sistema semplice ed immediato ha consentito la proliferazione di siti WEB.

Chiunque può fare il proprio sito, inserire e rendere pubbliche le informazioni che vuole.

Se nel 1994 le dimensioni complessive della Rete sono raddoppiate il Web si è moltiplicato di almeno 20 volte. In soli 18 mesi gli utilizzatori hanno creato più di 3 milioni di pagine che integrano informazioni, immagini e suoni, entertainment e pubblicità".

Il linguaggio utilizzato per la creazione di pagine web è l'HTML

L'HyperText Markup Language (HTML) (traduzione letterale: linguaggio di marcatura per ipertesti) è un linguaggio usato per descrivere la struttura dei documenti ipertestuali disponibili nel World Wide Web ossia su Internet. Tutti i siti web sono scritti in HTML, codice che viene letto ed elaborato dal browser, il quale genera la pagina che viene visualizzata sullo schermo del computer. L'HTML non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web. *Punto* HTML (.html) o *punto* HTM (.htm) è anche l'estensione comune dei documenti HTML. (wikipedia)

I Browser

Un **browser web** (in italiano: *navigatore*) è un programma che consente agli utenti di visualizzare e interagire con testi, immagini e altre informazioni, tipicamente contenute in una pagina web di un sito (o all'interno di una rete locale). Il browser è in grado di interpretare il codice HTML (e più recentemente XHTML) e visualizzarlo in forma di ipertesto. L'HTML è il codice col quale la maggioranza delle pagine web nel mondo sono composte: il web browser consente perciò la navigazione nel web. I browser solitamente vengono utilizzati su personal computer, ma non mancano altri dispositivi in grado di effettuare la navigazione con un browser, tra cui i palmari e gli smartphone.

2.6 INTERNET E MULTIMEDIALITA'

NON SOLO TESTO

Con il www Internet diventa multimediale: nelle pagine web è possibile infatti inserire animazioni, suoni, immagini, filmati e programmi;

Vedere un film, ascoltare musica, scambiare immagini sono azioni che rappresentano la realtà di oggi della rete e creano una vera e propria integrazione di mezzi e strumenti;

In poche parole creano un ambiente multimediale;

Multimedia: Il termine, conosciuto anche dai non addetti ai lavori, ha una definizione contestata: multimediale è l'integrazione su uno stesso supporto di dati di diversa natura (testi, suoni, immagini fisse o animate ecc..) visualizzati e gestiti tramite un computer che permette, attraverso programmi appositi, di interagire sulla rappresentazione delle informazioni: infatti la caratteristica fondamentale della multimedialità è proprio la possibilità di interagire con gli strumenti e i mezzi a disposizione.

In realtà il Multimedia nasce fuori dalla rete (off-line) e i primi prodotti multimediali sono stati prodotti su CDROM.

E' solo con l'avvento della rete (ON-LINE) che il multimedia è in grado di sfruttare tutte le sue potenzialità, soprattutto in termini di interattività.

Il futuro della rete è una integrazione sempre più spinta dei vari media, televisione, radio, immagini e computer

2.7 IL COMMERCIO ELETTRONICO

Uno dei fenomeni maggiori collegati ad Internet è l' **e-commerce**, cioè l'uso della rete per commercializzare e vendere prodotti di qualsiasi genere.

Attraverso l'E-commerce è possibile acquistare da casa qualunque bene o servizio utilizzando siti web predisposti ed eliminando molti passaggi intermedi tra il produttore e il consumatore.

Molti commentatori prevedono che l'E-commerce sarà l'unico modo di acquistare e vendere; probabilmente questa affermazione è esagerata ma, sicuramente, le aziende dovranno sempre di più fare i conti con questo fenomeno che non solo modificherà la vendita ma anche lo stesso rapporto con il mercato.

Marketplace e Il fenomeno eBay

Fondato il 6 settembre 1995, **eBay** è una piattaforma che offre ai propri utenti la possibilità di vendere e comprare oggetti sia nuovi che usati, in qualsiasi momento, da qualunque postazione Internet e con diverse modalità, incluse le vendite a prezzo fisso e a prezzo dinamico, comunemente definite come "aste online".

È obbligatoria l'iscrizione gratuita al sito. Qualunque acquirente può essere anche venditore dopo aver fatto una verifica tramite l'inserimento di un codice che eBay manda presso l'abitazione dello stesso oppure tramite il controllo con inserimento dei dati della carta di credito o di una carta prepagata.

Marketplace

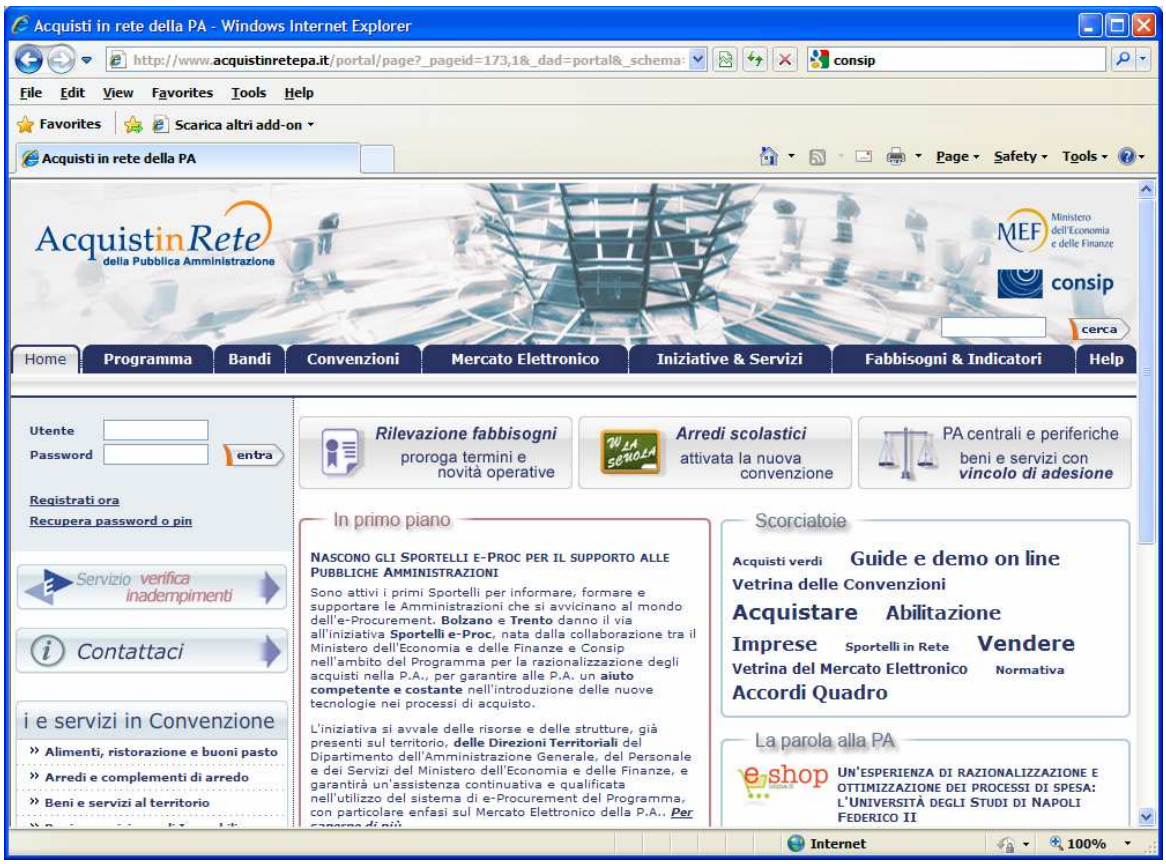
I marketplace sono, in generale, il luogo, reale o metaforico, in cui avvengono degli scambi. Nella lingua italiana, tuttavia, i marketplace servono ad indicare i siti internet di intermediazione per la compravendita di un bene o un servizio; in altre parole il marketplace, che in lingua inglese significa "luogo di mercato", è un mercato online in cui sono raggruppate le merci di diversi venditori o diversi siti web. L'esempio più noto di marketplace è eBay.

Anche la Pubblica Amministrazione ha realizzato un Programma per la Razionalizzazione degli Acquisti nella P.A., realizzato dal Ministero dell'Economia e delle Finanze tramite Consip S.p.A., nasce a seguito della Finanziaria 2000 con

l'obiettivo di ottimizzare gli acquisti pubblici promuovendo l'innovazione come leva del cambiamento.

Il Programma si inserisce nel più ampio quadro degli indirizzi di e-Governement: entro il 2010, secondo le direttive dell'UE, tutte le procedure di approvvigionamento delle Amministrazioni pubbliche dovranno transitare tramite strumenti telematici di acquisto. L'e-Procurement dovrà garantire una maggiore competitività della Pubblica Amministrazione europea e diminuire le distanze tecniche e organizzative esistenti tra gli stati membri.

Il portale di riferimento è: AcquistiInRetePA http://www.acquistinretepa.it



2.8 INTERNET PER LAVORO (ESEMPI DI POTENZIALITA')

- Lavorare con la posta elettronica;
- cercare le informazioni sulla rete e "scaricare" sul proprio computer i dati che interessano;
- pubblicare un proprio sito attraverso il quale mostrare la propria attività;
- interagire con siti esistenti allo scopo di fare domande specifiche,chiedere informazioni, prenotare biglietti ecc…;
- seguire corsi di formazione in rete;
- utilizzare strumenti di supporto al lavoro.

Nel mondo dell'informatica il **download** (in italiano, *scaricamento*) è l'azione di ricevere o prelevare dalla rete (es. da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'utente. Nella maggior parte dei casi il download di un file è la conseguenza di una richiesta, più o meno trasparente all'utente del sistema.

Ogni volta che un computer connesso ad internet richiede una pagina o un qualsiasi contenuto su internet, un computer remoto invia l'oggetto richiesto attraverso una rete di calcolatori fino al computer che aveva inviato la richiesta, il quale riceve i dati sotto forma di pacchetti da ricostruire. All'interno di questo meccanismo la parte di richiesta di download, che pure prevede l'invio di informazioni al sistema remoto, non può essere definita upload. Per questo motivo il download di un file comporta necessariamente anche l'utilizzo di parte di banda dell'upload; nel caso in cui la banda in upload sia satura la velocità del download si autolimiterà. (wikipedia)

Queste sono solo alcune tra le infinite potenzialità di internet, che sta diventando strumento insostituibile per qualunque azienda, ufficio o professionista.

Anche la P.A. è coinvolta in questo fenomeno e l'uso della rete offre enormi opportunità non solo in termini di maggiore efficienza per l'attività lavorativa ma anche per la comunicazione con il cittadino.

Alcuni tra i siti di maggiore interesse per la P.A. sono:

- Centro Nazionale per l'Informatica nella Pubblica Amministrazione
http://www.cnipa.gov.it/site/it-IT/
- Camera dei Deputati
http://www.camera.it/
- Consiglio Nazionale delle Ricerche
http://www.cnr.it/
- Corpo Forestale dello Stato
http://www.corpoforestale.it/
- Dipartimento della Funzione Pubblica
http://www.funpub.it/
- Dipartimento della Protezione Civile
http://www.protezionecivile.it/
- Dipartimento per gli Affari Sociali
http://www.affarisociali.it/
- ENEA
http://www.enea.it
- Istituto Nazionale di Statistica (ISTAT)
http://www.istat.it/
- Istituto Poligrafico dello Stato
http://www.ipzs.it/
- Istituto Superiore di Sanità
http://www.iss.it

MINISTERI
Affari Esteri

Piazzale della Farnesina, 1 - 00194 ROMA
Tel: (+39) 06.36911
Sito: www.esteri.it
Modulo richiesta informazioni
Interno
Palazzo Vicinale
Via Agostino Depretis 7, 00184 ROMA
Tel: (+39) 06.4651
Tel. Ufficio stampa: +39 0646533777
Sito: www.interno.it
E-mail: Per contattare il ministero via e-mail

Giustizia

Via Arenula, 70 - 00186 ROMA
Tel: (+39) 06.68851
Sito: www.giustizia.it
E-mail: callcenter@giustizia.it

Difesa

Gabinetto - Via XX Settembre, 8 - 00187 ROMA Tel: (+39) 06.4882126/7
Palazzo dell'Esercito - Via XX Settembre, 123

- 00187 ROMA Tel: (+39) 06.47351
- Palazzo della Marina - Piazza della Marina
- - 00196 ROMA Tel: (+39) 06.36801
- Palazzo dell'Aeronautica - Viale dell'Università, 4
- - 00187 ROMA Tel: (+39) 06.49861
- Sito: www.difesa.it
- E-mail: spi.ca@gabmin.difesa.it
- pi@smd.difesa.it

Economia e Finanze

Via XX Settembre, 97 - 00187 ROMA
Tel: (+39) 06.47611
Tel. Ufficio Stampa: (+39) 06.47614606
E-mail: ufficio.stampa@tesoro.it
Siti: www.mef.gov.it
www.tesoro.it

Dipartimento delle Finanze

Agenzia delle Entrate
Agenzia delle Dogane
Agenzia del Territorio
Agenzia del Demanio
E-mail: coordinamento.portale@tesoro.it
dpf.comist@finanze.it

Sviluppo economico

Gabinetto del Ministro - Via Molise, 2 - 00187 ROMA
tel: (+39) 06.42043486 -06.420434000
fax: (+39) 06.47887964
Ufficio stampa: (+39) 06.420434315 - 47887859 - fax (+39) 06.47887878

Sito: www.sviluppoeconomico.gov.it
E-mail: Segreteria.ministro@sviluppoeconomico.gov.it
Commercio internazionale
Viale Boston 25 - 00144 ROMA
Tel: (+39) 06.59931
URP: (+39) 0659932800
Sito: www.mincomes.it
E-mail: info@mincomes.it
urp@mincomes.it
Comunicazioni
Eur, Viale America, 201 - 00144 ROMA
Tel: (+39) 06.54441
Sito: www.comunicazioni.it
E-mail: ufficio.stampa@comunicazioni.it
urpcom@comunicazioni.it
Politiche Agricole, Alimentari e Forestali
Via XX Settembre, 20 - 00187 ROMA
Tel: (+39) 06.46651
Sito: www.politicheagricole.gov.it
E-mail: ufficiostampa@politicheagricole.gov.it
urp@politicheagricole.gov.it
internet.redazione@politicheagricole.gov.it
Ambiente, Tutela del Territorio e del Mare
Viale Cristoforo Colombo, 44 - 00147 ROMA
Tel: (+39) 06.57221
Sito: www.minambiente.it
E-mail: segr.ufficiostampa@minambiente.it
Infrastrutture e Trasporti
Piazzale Porta Pia, 1 - 00198 ROMA
Tel: (+39) 06.44121
Sito: www.infrastrutture.gov.it
E-mail: ufficio.stampa@infrastrutture.gov.it
urplp@infrastrutture.gov.it
Piazza della Croce Rossa 1- 00187 ROMA
Sito: www.trasporti.gov.it
Lavoro, Salute e Politiche Sociali
Via Veneto 56 - 00187 ROMA
Tel:(+39) 06.481611
Ufficio stampa: (+39) 0648161451-2
Sito: www.lavoro.gov.it
E-mail: ufficiostampa@lavoro.gov.it
Via Giorgio Ribotta 5 - 00144 Roma
Tel. (+39) 06.5994.1
Sito: www.ministerosalute.it
E-mail: ufficiostampa@sanita.it
E-mail: urpminsalute@sanita.it

Via Fornovo, 8 - 00192 ROMA
Tel: (+39) 06.36751
Sito: www.solidarietasociale.gov.it
Istruzione, Università e Ricerca
Piazzale Kennedy, 20 - 00144 ROMA
Tel: (+39) 06.58491
Sito: www.miur.it
E-mail: ufficio.stampa@miur.it
Viale Trastevere, 76/a - 00153 ROMA
Tel: (+39) 06.58491
Sito: www.pubblica.istruzione.it
E-mail: uffstampa@istruzione.it
E-mail: urp@istruzione.it
(+39) 06 58492377
Beni e Attività Culturali
Via del Collegio Romano, 27 - 00186 ROMA
Tel: (+39) 06.67231
Sito: www.beniculturali.it
E-mail: urp@beniculturali.it
ufficiostampa@beniculturali.it

2.9 E-MAIL

Una delle applicazioni più interessanti e potenzialmente più vicine all'utente di internet è la **posta elettronica**.

Con **l'E-mail** è possibile scambiare messaggi, file di testo e informazioni di qualunque tipo. Naturalmente se tali informazioni sono su supporto digitale.

La posta elettronica è il metodo di spedizione ultrarapida a bassissimo costo (e in tempi molto ridotti) di messaggi via computer. Per poter utilizzare un'E-mail è necessario utilizzare un programma specifico e di potersi collegare in rete. Ad ogni utente viene assegnato un indirizzo di e-mail univoco e valido per tutto il mondo che rappresenta il suo "biglietto da visita" nel mondo di Internet.

Ogni casella e-mail ha un indirizzo specifico, composto nel seguente modo: **utente@dominio.it** dove il carattere @, chiamato comunemente "AT" *chiocciola*, separa il nome dell'utente dall'identificativo del *provider* ed it è l'identificativo del paese d'origine (in questo esempio l'Italia).

I protocolli utilizzati nello scambio della posta elettronica sono:

- **SMTP** (Simple Mail Transfer Protocol) per l'invio dei messaggi;
- **POP3** (Post Office Protocol) per la ricezione dei messaggi (in alternativa alcuni provider utilizzano il protocollo IMAP – Internet Message Access Protocol).

La posta elettronica ha cambiato il modo di comunicare negli ultimi decenni. Comunicazione in tempo reale, risparmio di spesa, possibilità di comunicare "uno a molti" sono fattori di indubbio vantaggio per la società moderna. Basti pensare proprio alla possibilità di sfruttare i campi Cc e Bcc che permettono, rispettivamente di inserire più nominativi e-mail in Copia carbone (Carbon copy) o in Copia Carbone nascosta (Blind Carbon Copy). In quest'ultimo caso tutti gli

utenti inseriri riceveranno il messaggio ma non saranno a conoscenza degli indirizzi degli altri quindi dell'invio della stessa e-mail a più utenti.

2.10 LA COMUNICAZIONE SU INTERNET, BLOG, PODCAST

Prima di affrontare il capitolo relativo alle applicazioni possibili grazie alla rete Internet, vediamo di comprendere tipologia e significato di alcune sigle riferite alla modalità e velocità di connessione alla rete.

Per collegarsi ad Internet è necessario procurarsi un ***account,*** richiedendolo ad un **Provider** (ISP).

Un **Internet Service Provider** (in sigla **ISP**), o **fornitore d'accesso**, o, se è chiaro il contesto informatico, anche semplicemente **provider**, è una struttura commerciale o un'organizzazione che offre agli utenti (residenziali o imprese) accesso a Internet con i relativi servizi. (Wikipedia)

RTC

Il metodo più semplice ed economico per un utente privato che desidera collegarsi ad Internet, invece, è quello di utilizzare la **Rete Telefonica Commutata**. La RTC è la normale rete telefonica nata per trasportare la voce e non l'enorme quantità di dati che oggi viaggia in rete.

In particolare per collegarsi ad un Provider tramite RTC, si inserisce un **modem** tra l'uscita seriale del PC o la presa USB e la presa telefonica di casa.

Fino a qualche anno fa i modem più veloci erano in grado di funzionare a 1.200bps o, al massimo, a 2.400bps. Si doveva, però, fare i conti con i disturbi della linea telefonica analogica che riduceva drasticamente l'efficienza di trasmissione. Oggi, invece, con il miglioramento della qualità delle linee e con la disponibilità di modem a 56.000bps, aventi circuiti per la compressione dei dati e la correzione automatica degli errori, è possibile comunicare a velocità anche superiore a 4-5Kbyte al secondo se il traffico telefonico nella Rete ce lo consente. Ovviamente questo tipo di soluzione è comunque impensabile qualora si vogliano visualizzare filmati e/o veicolare file di grandi dimensioni.

Il collegamento al provider dell'utente remoto tramite rete telefonica commutata (**RTC**) è detto connessione **dial-up.**

Per accedere ad Internet non servono oggi grandi competenze informatiche; rispetto a qualche anno fa le procedure sono state grandemente semplificate.

Precedentemente alle linee ADSL che permettono di trasferire dati ad alta velocità pur usufruendo della linea telefonica, si utilizzavano i **modem,** apparati che permettevano il collegamento ad Internet (ma non solo, prima ancora cerano i BBS) attraverso la rete telefonica.

La parola **modem** significa **mo**dulatore-**dem**odulatore e permette per l'appunto di trasformare il segale analogico della linea telefonica in segnale digitale e viceversa. La velocità di trasmissione dati è però bassa e non permette la migliore visualizzazione di filmati ed animazioni su Internet

Oggi questa soluzione è ancora adottata nelle località non raggiunte dalle linee **ADSL**.

ISDN

In taluni casi si utilizzano ancora le linee ISDN (**Integrated Services Digital Network)**, un servizio di telefonia digitale disponibile su abbonamento nelle aree coperte dal servizio. Più specificamente, l'ISDN è un protocollo che descrive l'effettuazione delle chiamate e la relativa terminazione; la velocità delle postazioni di lavoro delle scuole è al massimo di 128 Kb al secondo.

ADSL

La tecnologia **ADSL** (acronimo dell'inglese **Asymmetric Digital Subscriber Line**), appartenente alla famiglia di tecnologie denominata DSL, permette l'accesso ad Internet ad alta velocità (si parla di banda larga o *broadband*). La velocità di trasmissione va dai 640 kilobit per secondo (kb/s) in su, a differenza dei modem tradizionali di tipo dial-up, che consentono velocità massime di 56 kb/s in download e 48 kb/s in upload (standard V.92), e delle linee ISDN che arrivano fino a 128 kb/s (utilizzando doppio canale a 64 kb/s) simmetrici.

Con l'ADSL il segnale è codificato in maniera digitale anche nella parte dalla linea telefonica lato utente (*"subscriber line"*) **e la velocità di invio dati è asimmetrica**. Quella in uscita infatti è più bassa, per suddividere meglio la quantità di informazione a disposizione, tenendo conto che tipicamente per le utenze private si chiede molta più informazione in ingresso che in uscita.

Peculiarità della tecnologia ADSL è la possibilità di usufruirne senza dover cambiare i cavi telefonici esistenti e senza dover usare linee separate per i dati e per le comunicazioni-voce normali: sul doppino telefonico in rame, è infatti possibile far viaggiare contemporaneamente sia i dati digitali che il segnale telefonico analogico. (Wikipedia).

HDSL

HDSL (acronimo inglese di *High data rate Digital Subscriber Line*) è la prima tecnologia della famiglia xDSL, nata 30 anni fa per potenziare la velocità delle connessioni Internet su tradizionale doppino telefonico (due fili di rame). Consente di raggiungere velocità fino a 8 Mb/s **sincroni** (sia in download che in upload) con una connessione sempre attiva. Perciò richiede un *router* V.35 (molto costoso) collegato a un *router*. Esiste soltanto per traffico dati e non per quello voce. (Wikipedia)

Con la linea HDSL è quindi possibile **fornire** anche 'servizi' web e VoIP

Digital Divide

La possibilità di avere un collegamento alla rete Interne veloce o meno ha posto all'attenzione il fenomeno del **Digital Divide**.

Con **Digital Divide** (**divario digitale**, spesso abbreviato in **DD**) si intende il divario esistente tra chi può accedere alle nuove tecnologie (internet, personal computer) e chi no. Le cause sono ad oggi oggetto di studio. Tuttavia vi è consenso nel riconoscere che condizioni economiche, di istruzione e, in molti paesi, l'assenza di infrastrutture siano i principali motivi di esclusione.

ALCUNE TRA LE POTENZIALITA' COMUNICATIVE DI INTERNET SONO…

E-MAIL	scambio di informazioni uno ad uno
CHAT	discussioni di gruppo in tempo reale
MAILING LIST	gruppi di discussioni su Internet
VIDEOCONFERENZA	conferenza a distanza con video e audio
SITOWEB	scambio di informazioni (accedere a siti per fornire informazioni, costruire un proprio sito per fornire informazioni)
E-LEARNING	Per **e-learning** si intende la possibilità di imparare sfruttando la rete internet e la diffusione di informazioni a distanza. L'e-learning non è limitato alla formazione scolastica, essendo rivolto anche a utenti adulti, studenti universitari, insegnanti, ecc. ed anche nella formazione aziendale, specialmente per le organizzazioni con una pluralità di sedi.
BLOG	un **blog** è un sito internet, generalmente gestito da una persona o da una struttura, in cui l'autore scrive periodicamente – *in modo facilitato, senza particolari competenze informatiche* - come in una sorta di **diario on-line**, inserendo opinioni personali, descrizione di eventi, o altro materiale come immagini o video. Ogni aggiornamento è generalmente inserito in ordine cronologico inverso. Il termine *blog* è la contrazione di *web-log*, ovvero "traccia su rete"
PODCAST	Il **podcasting** è un sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati *podcast*, utilizzando un programma ("client") generalmente gratuito

	chiamato *aggregatore* o *feed reader*. Un **podcast** è perciò un file (generalmente audio o video), messo a disposizione su Internet per chiunque si abboni ad una trasmissione periodica e scaricabile automaticamente da un apposito programma, chiamato **aggregatore**, e si basa sui **feed RSS**

2.11 LA FORMAZIONE ON-LINE

CMS, LMS, LCMS

Gli strumenti attraverso i quali vengono erogati on-line i corsi in modalità e-Learning possono essere di diverso tipo: CMS, LMS, LCMS, Piattaforme collaborative, Authoring tools, strumenti audiovisivi, strumenti di simulazione, strumenti di testing e valutazione. Gli strumenti più completi, che racchiudono più funzionalità in quanto spesso integrati, sono i LCMS.

CMS

Un content management system (spesso abbreviato in CMS), letteralmente *sistema di gestione dei contenuti*, è uno strumento software installato su un server web studiato per facilitare la gestione dei contenuti di siti web, svincolando l'amministratore da conoscenze tecniche di programmazione.

Esistono CMS specializzati, cioè appositamente progettati per un tipo preciso di contenuti (un'enciclopedia on-line, un blog, un forum, ecc.) e CMS generici, che tendono ad essere più flessibili per consentire la pubblicazione di diversi tipi di contenuti.

Tecnicamente un CMS è un'applicazione lato server, divisa in due parti: la sezione di amministrazione (*back end*), che serve ad organizzare e supervisionare la produzione dei contenuti, e la sezione applicativa (*front end*), che l'utente web usa per fruire dei contenuti e delle applicazioni del sito.

I CMS possono essere programmati in vari linguaggi tra cui più comunemente in PHP e ASP; il tipo di linguaggio adoperato è indifferente a livello di funzionalità. I CMS in PHP sono multipiattaforma, mentre i CMS in ASP possono essere utilizzati solo su piattaforme Windows. (Wikipedia)

LMS

Un learning management system (LMS) è la piattaforma applicativa (o insieme di programmi) che permette l'erogazione dei corsi in modalità e-learning. Il learning management system presidia la distribuzione dei corsi on-line, l'iscrizione degli studenti, il tracciamento delle attività on-line. Gli LMS spesso operano in associazione con gli LCMS (learning content management

system) che gestiscono direttamente i contenuti, mentre all'LMS resta la gestione degli utenti e l'analisi delle statistiche.

La maggior parte dei LMS sono strutturati in maniera tale da facilitarne, dovunque e in qualunque momento, l'accesso e la gestione dei contenuti.

Normalmente un LMS consente la registrazione degli studenti, la consegna, la frequenza ai corsi e-learning e una verifica delle conoscenze.

In un sistema LMS più completo si possono anche trovare strumenti quali l'amministrazione di competenza, l'analisi di abilità, la pianificazione di successione, le certificazioni, i codici categoria virtuali e la ripartizione delle risorse (sedi della riunione, stanze, manuali, istruttori, ecc.). La maggior parte dei sistemi tengono conto dello studente principiante, facilitandone l'auto-iscrizione e l'accesso ai corsi. (Wikipedia).

LCMS

Il learning content management system (LCMS) è un modulo software presente nelle piattaforme di e-learning che riunisce tutte le funzionalità necessarie alla gestione dei contenuti per l'insegnamento on-line, come ad esempio:

- Creazione, gestione e memorizzazione dei contenuti didattici;
- Composizione e modularizzazione delle unità didattiche fondamentali, chiamate learning object (LO);
- Tracciamento e memorizzazione delle interazioni degli studenti con i learning object.

Un LCMS gestisce l'importazione e la pubblicazione dei learning object, "pacchetti" indipendenti in grado di soddisfare uno o più obiettivi didattici. (Wikipedia)

Le principali caratteristiche che un LCMS deve possedere per supportare efficacemente i processi formativi di una organizzazione sono riconducibili alle seguenti funzionalità:

- Desktop personale con il link ai corsi frequentati, ai gruppi di appartenenza, a chat, forum;
- Sistemi di gestione dei corsi;
- Ambiente di formazione con attività di testing & assessement, glossari, download, funzioni di stampa, libri digitali, appunti;
- Sistemi di comunicazione come chat, forum e messaggistica;
- Sistemi di gruppo per il lavoro collaborativo e l'organizzazione degli utenti e delle risorse;
- Ambiente integrato per la creazione di contenuti a prescindere dalle conoscenze di HTML;
- Modulazione dei percorsi didattici sulla base degli obiettivi fissati: a seconda delle esigenze dei formatori e del feedback degli utenti, è possibile aggiungere nuovi elementi o modificare quelli esistenti creando corsi in continua evoluzione;
- Interfaccia Utenti e per l'Amministrazione del sistema;
- Interfaccia multilingue;

- Supporto dei principali standard per la gestione e creazione di contenuti e-learning (AICC, IMS, SCORM);
- Sistema di tracciamento degli utenti.

Learning Object

Un learning object (sinteticamente noto come LO dal relativo acronimo) è una unità di istruzione per l'e-learning, riutilizzabile.

I learning objects costituiscono particolari tipi di risorse di apprendimento autoconsistenti, dotate di modularità, reperibilità, riusabilità e interoperabilità, che ne consentono la possibilità di impiego in contesti diversi.

Lo sviluppo delle nuove tecnologie dell'informazione e della comunicazione ha avuto significative ripercussioni anche sulle modalità di apprendimento, stimolando la formazione di nuove risorse didattiche.

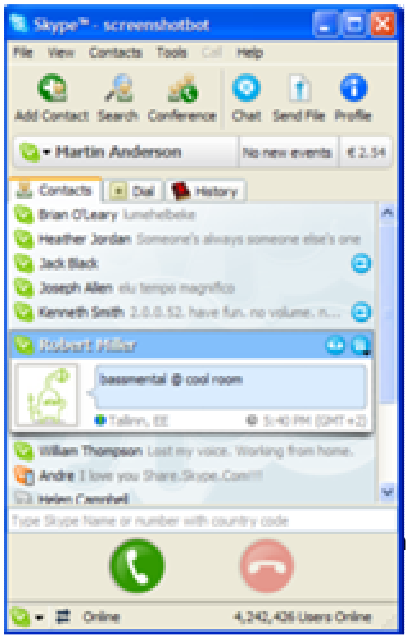
A questo proposito, spesso si ritiene che l'approccio pragmatico/produttivo dell'e-learning, finalizzato al risparmio di tempi e costi nella fase di progettazione e produzione dei materiali didattici, sia l'orientamento fondante che ne ha la realizzazione di LO. (Wikipedia)

SCORM

Lo SCORM definisce, nell'e-Learning, le specifiche relative al riutilizzo, tracciamento e catalogazione degli oggetti didattici (learning object), i "mattoni elementari" con i quali vengono strutturati i corsi. La piattaforma di e-learning ha solo il compito di dialogare con l'oggetto, interpretando i messaggi che gli vengono passati. Ciò è possibile in quanto SCORM definisce al suo interno le caratteristiche che dovrebbero essere supportate dal Learning Management System (LMS). La compatibilità della piattaforma si rende necessaria solamente per "capire la lingua" dell'oggetto e, se necessario, per potergli rispondere. (Wikipedia).

Comunicazione sincrona e asincrona

La possibilità di effettuare videoconferenze a distanza rappresenta sicuramente uno degli aspetti potenzialmente più produttivi per l'utilizzo lavorativo di Internet. La videoconferenza è infatti in grado di mettere in collegamento persone situate fisicamente il luoghi differenti e di farle comunicare visivamente in tempo reale, con grandi risparmi in termini di costi e miglioramento dell'efficienza.



Alcuni degli applicativi che abbiamo visto permettono dunque una comunicazione "differente" rispetto ad altri. La sostanziale diversità è insita nella tipologia di comunicazione: "sincrona", ovvero in tempo reale ed è quindi richiesta la presenza di un altro utente al PC nello stesso momento (chat, VoIP, instant messaging); "asincrona", ovvero in differita dove non è richiesta la presenza di un altro utente al PC nello stesso momento in quanto il

messaggio può essere letto in un secondo tempo (mail, mailing-list, forum).

Skype

Skype è un software proprietario freeware di messaggistica istantanea e VoIP. Esso unisce caratteristiche presenti nei *client* più comuni (chat, salvataggio delle conversazioni, trasferimento di file) ad un sistema di telefonate basato su un network *Peer-to-peer*.

La possibilità di far uso di un servizio a pagamento, SkypeOut, che permette di effettuare chiamate a telefoni fissi, rendono il programma competitivo rispetto ai costi della telefonia tradizionale, soprattutto per le chiamate internazionali e intercontinentali. Con Skype è possibile anche inviare sms a basso costo verso tutti gli operatori di rete mobile.

2.12 MOTORI DI RICERCA

La rivoluzione Internet non può considerarsi tale senza prendere in considerazione lo sviluppo dei motori di ricerca: Altavista, Arianna e il più famoso Google.

Un motore di ricerca è un sistema automatico che analizza un insieme di dati spesso da lui stesso raccolti e restituisce un indice dei contenuti disponibili classificandoli in base a formule matematiche che ne indichino il grado di rilevanza data una determinata chiave di ricerca.

E' importante conoscere le corrette modalità d ricerca per guadagnare tempo ed ottenere risultati attendibili.

Gli operatori logici

L'obiettivo della ricerca avanzata è quello di permettere un interrogazione abbastanza specifica, in modo da escludere documenti non rilevanti. Per fare questa selezione è necessario definire il maggior numero possibile di caratteristiche che il documento che stiamo cercando deve possedere, più specifica è la descrizione, meno sono i documenti che vi corrispondono, e più pertinente è il loro contenuto

Gli operatori logici o booleani prendono il loro nome da George Boole, matematico inglese della prima metà dell'800 che formalizzo la logica binaria che sta alla base dei moderni calcolatori. I principali e più diffusi sono AND, OR, e NOT, a cui si può aggiungere negli strumenti di ricerca NEAR.

Due o più parole legate da NEAR devono comparire entrambe nel testo e a distanza ravvicinata (tipicamente a distanza massima di 10 parole).

Una parola chiave preceduta da AND NOT indica al motore di ricerca che non vogliamo i documenti che contengono quella parola.

Se i risultati sono troppi, oppure non ci vengono in mente che parole generiche, possiamo cominciare ad aggiungere parole chiave legate da AND. Un modo alternativo per scremare i risultati è l'uso di NOT. Se facendo così abbiamo ridotto troppo il campo della ricerca si può utilizzare OR per allargarlo leggermente. Procedendo per aggiustamenti successivi, utilizzando se necessario le *parentesi*, mettendo o togliendo parole chiave per mezzo di AND o ponendo

alternative per mezzo di OR, si riesce in genere a ridurre i risultati ad un piccolo numero veramente rilevante.

2.13 RIEPILOGO

aumenta in maniera esponenziale le capacità di comunicazione	e-mail, chat, mailing list, videoconferenza ecc
fornisce un archivio di informazioni praticamente inesauribile, aggiornabile e facilmente consultabile	siti web
fornisce la possibilità di mostrare la propria attività	sito web
modifica le stesse procedure di lavoro e i rapporti tra le organizzazioni	e-mail, siti web, chat, ecc…

Per accedere ad Internet non servono oggi grandi competenze informatiche; rispetto a qualche anno fa le procedure sono state grandemente semplificate.

Precedentemente alle linee ADSL che permettono di trasferire dati ad alta velocità pur usufruendo della linea telefonica, si utilizzavano i **modem**, apparati che permettevano il collegamento ad Internet (ma non solo, prima ancora cerano i BBS) attraverso la rete telefonica.

La parola modem significa **mo**dulatore-**dem**odulatore e permette per l'appunto di trasformare il segale analogico della linea telefonica in segnale digitale e viceversa. La velocità di trasmissione dati è però bassa e non permette la migliore visualizzazione di filmati ed animazioni su Internet

Oggi questa soluzione è ancora adottata nelle località non raggiunte dalle linee ADSL. In taluni casi si utilizzano ancora le linee ISDN (**Integrated Services Digital Network**), un servizio di telefonia digitale disponibile su abbonamento nelle aree coperte dal servizio. Più specificamente, l'ISDN è un protocollo che descrive l'effettuazione delle chiamate e la relativa terminazione; la velocità delle postazioni di lavoro delle scuole è al massimo di 128 Kb al secondo.

La possibilità di avere un collegamento alla rete Interne veloce o meno ha posto all'attenzione il fenomeno del Digital Divide

Con **Digital Divide** (divario digitale, spesso abbreviato in DD) si intende il divario esistente tra chi può accedere alle nuove tecnologie (internet, personal computer) e chi no. Le cause sono ad oggi oggetto di studio. Tuttavia vi è consenso nel riconoscere che condizioni economiche, di istruzione e, in molti paesi, l'assenza di infrastrutture siano i principali motivi di esclusione.

Molti sono i progetti di tipo sociale, economico, tecnologico e culturale per contrastare il fenomeno del dgital-divide: uno per tutti:

OLPC

One Laptop Per Child (la cui sigla è OLPC) è un'organizzazione non-profit creata per sovraintendere al progetto del computer da 100 dollari, $100 laptop. "One Laptop Per Child" ha guadagnato molta attenzione dopo che Nicholas Negroponte e Kofi Annan hanno mostrato un prototipo funzionante dal valore di $100.

L'iniziativa è volta alla progettazione, produzione e distribuzione di laptop da 100 dollari per fornire a ogni bambino del mondo, specie a quelli nei paesi in via di sviluppo, l'accesso alla conoscenza e alle moderne forme educative. I laptop presentati dal team di Negroponte sono basati su programmi open source, processore low-cost Geode e possono essere alimentati con batteria interna ricaricabile con una manovella per la ricarica, batteria auto, trasformatore di rete.

In Italia esiste un'esperienza interessante a Torino denominata: Un computer nello zianetto http://share.dschola.it/olpc/default.aspx

Il portatile a basso costo JumPC di Olidata ha schermo da 7 pollici e peso di un chilo e mezzo, semplice, funzionale e dalle dimensioni contenute. Tecnicamente è un derivato dell'Intel Classmate di seconda generazione, un laptop a basso costo destinato alla prima informatizzazione dei bambini nei Paesi in Via di Sviluppo, e pertanto può essere classificato nella cateogoria dei netbook o degli OLPC.

Netiquette

http://www.pubblica.istruzione.it/posta_docenti/netiquette.pdf

Esiste un insieme di regole denominato Netiquette che si potrebbe tradurre in "Galateo (Etiquette) della Rete (Net)" che consiste nel rispettare e conservare le risorse di rete e nel rispettare e collaborare con gli altri utenti.

Ergonomia

L'ergonomia (dal greco ergos = *lavoro* e nomos = *controllo*) è una disciplina che persegue la progettazione di prodotti, ambienti e servizi adatti alle necessità dell'utente, migliorando la sicurezza, la salute, il comfort, il benessere e la prestazione umana. Si tratta di una scienza interdisciplinare che coinvolge l'anatomia, l'ingegneria, la biologia, la fisiologia, la psicologia, l'ambiente di lavoro, ecc. Il suo obiettivo (sancito dal D.L.vo 81/2008 Testo Unico sulla Sicurezza nei luoghi di Lavoro) è di stabilire le soluzioni in grado di tutelare la salute del lavoratore, nella sua interazione con le macchine e l'ambiente, e di conseguenza accrescere l'efficienza e la sicurezza sul posto di lavoro, garantendo quindi l'integrità fisica e psicologica del lavoratore e potenziandone le capacità operative.

Gli studi sull'ergonomia del posto di lavoro sostengono che:

- lo schermo deve consentire una facile lettura e deve essere orientabile a seconda delle esigenze dell'utente, deve avere uno schermo filtrante e posizionato a circa 60 cm dall'occhio;
- la tastiera deve essere inclinabile e distante dallo schermo;

- il mouse deve essere vicino all'utente e deve essere poggiato su un tappetino;
- il tavolo di lavoro deve essere abbastanza grande da permettere all'utente di appoggiarci le braccia;
- la sedia deve essere regolabile e deve avere un appoggio a cinque razze munite di rotelle per essere spostata facilmente.

Anche chi non si sente portato o non prova alcun interesse verso la rete è bene faccia degli sforzi e cerchi di superare la diffidenza.

Oggi non è più possibile farne a meno!

2.14 RESENTE E FUTURO

Anche chi non si sente portato o non prova alcun interesse verso la rete è bene faccia degli sforzi e cerchi di superare la diffidenza.

Oggi non è più possibile farne a meno!

Le enormi potenzialità espresse dalla rete internet, dai nuovi linguaggi comunicativi, dalle aumentate possibilità di collegamento alla rete anche di Paesi "poveri" o sino ad oggi non collegati per motivi diversi, l'interazione sempre più spinta con la televisione fa' sì che gli scenari presenti e futuri mutino rapidamente evolvendosi ulteriormente.

L'evoluzione tecnologica è un dato inarrestabile, e bisogna fare i conti con essa.

Sempre più spesso si parla di e-Book, di web semantico, di social network di integrazione internet-TV, di domotica, di web virtuale e avatar e altro ancora con sviluppi e scenari tutti da scoprire!

eBook

Un eBook (anche chiamato *e-book* oppure *ebook*) è un libro in formato elettronico (o meglio digitale). Il termine deriva dalla contrazione delle parole inglesi *electronic book*, viene utilizzato sia per indicare la conversione in digitale di una qualsiasi pubblicazione sia il dispositivo con cui il libro può essere letto.

Sino ad oggi era possibile scaricare da internet un testo nel proprio computer, ma la cosa presentava molti ostacoli per i lettori e per gli editori. Prima di tutto per leggerlo ci si doveva sedere davanti al video posto sul tavolo della propria abitazione e comunque la lettura prolungata stancava; in secondo luogo era quasi impossibile proteggere il diritto d'autore e una volta che il libro veniva messo in rete poteva essere duplicato al'infinito. Gli e-books risolveranno questi problemi: si potranno mettere in tasca o in borsetta ed essere letti dappertutto, sia di giorno che di notte; potranno contenere molti testi, molti romanzi protetti dalla duplicazione, ma soprattutto i romanzi costerano meno e quindi, come ha annunciato Bill Gates: *gli e-books determineranno il più grosso fattore di accelazione della cultura dopo Gutenberg.*

Si potrà studiare attraverso i corsi delle migliori Università, si potranno leggere libri, si potranno esplorare turisticamente luoghi e città. Il tutto con un libro elettronico tascabile che puoi tenere in mano e leggere in treno, in tram e in qualsiasi momento libero.

Internet TV

E' l'integrazione della TV in Internet.

Programmi televisivi, canali aggiuntivi e tematici, il tutto veicolato sulla reti ad alta velocità (talvolta su fibra digitale).

Social Network

Una rete sociale (spesso si usa il termine inglese *social network*) consiste di un qualsiasi gruppo di persone connesse tra loro da diversi legami sociali, che vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari. Le reti sociali sono spesso usate come base di studi interculturali in sociologia e in antropologia.

La versione di Internet delle reti sociali è una delle forme più evolute di comunicazione in rete, ed è anche un tentativo di violare la "regola dei 150". La rete delle relazioni sociali che ciascuno di noi tesse ogni giorno, in maniera più o meno casuale, nei vari ambiti della nostra vita, si può così "materializzare", organizzare in una "mappa" consultabile, e arricchire di nuovi contatti.

Il fenomeno delle social network nacque negli Stati Uniti e si è sviluppato attorno a tre grandi filoni tematici: l'ambito professionale, quello dell'amicizia e quello delle relazioni amorose.

L'esempio maggiormente diffuso ed esploso in questi ultimi du e anni è face book (www.facebook.com).

Web semantico

Con il termine web semantico, termine coniato dal suo ideatore, Tim Berners-Lee, si intende la trasformazione del World Wide Web in un ambiente dove i *documenti* pubblicati (pagine HTML, file, immagini, e così via) siano associati ad informazioni e dati (metadati) che ne specifichino il contesto semantico in un formato adatto all'interrogazione, all'interpretazione e, più in generale, all'elaborazione automatica.

Con l'interpretazione del contenuto dei documenti che il Web Semantico propugna, saranno possibili ricerche molto più evolute delle attuali, basate sulla presenza nel documento di parole chiave, ed altre operazioni specialistiche come la costruzione di reti di relazioni e connessioni tra documenti secondo logiche più elaborate del semplice link ipertestuale. (Wikipedia).

Second Life

Second Life è un mondo virtuale tridimensionale multi-utente online inventato nel 2003 dalla società americana Linden Lab. Il sistema fornisce ai suoi utenti (definiti "residenti") gli strumenti per aggiungere e creare nel "mondo virtuale" di *Second Life* nuovi contenuti grafici: oggetti, fondali, fisionomie dei personaggi, contenuti audiovisivi, ecc. La peculiarità del mondo di *Second Life* è quella di lasciare agli utenti la libertà di usufruire dei diritti d'autore sugli oggetti che essi creano, che possono essere venduti e scambiati tra i "residenti" utilizzando una moneta virtuale (il *Linden Dollar*) che può essere convertito in veri dollari statunitensi e anche in euro. (Wikipedia).

Esiste, nelle Aziende e nella PA in genere, l'altra faccia della medaglia; ovvero la problematica che molti dipendenti passano parte del loro tempo su Second Life e Facebook durante la normale attività lavorativa. Come e cosa fare?

Avatar

L'avatar è un'immagine scelta per rappresentare la propria utenza in comunità virtuali, luoghi di aggregazione, discussione, o di gioco on-line. La parola, che è in lingua sanscrita, è originaria della tradizione induista, nella quale ha il significato di incarnazione, di assunzione di un corpo fisico da parte di un dio (Avatar: "Colui che discende"): per traslazione metaforica, nel gergo di internet si intende che una persona reale che scelga di mostrarsi agli altri, lo faccia attraverso una propria rappresentazione, un'incarnazione: un *avatar* appunto.

Tale immagine, che può variare per tema e per grandezza (di solito stabilite preventivamente dai regolamenti delle *comunità virtuali*), può raffigurare un personaggio di fantasia (ad es. un cartone animato, un fumetto), della realtà (ad es. il proprio cantante o attore preferito, o anche la propria immagine), o anche temi più vari, come vignette comiche, testi, ed altro.

Il luogo di maggiore utilizzo degli *avatar* sono i forum, i programmi di instant messaging, e i giochi di ruolo on-line dove è d'uso crearsi un *alter ego*. Alcuni siti invitano a dotarsi di un avatar ispirato a un certo tema per renderne uniforme l'utilizzo in modo da migliorare il senso di appartenenza alla comunità virtuale. Per esempio il sito del Villaggio di Ofelon richiede un avatar di ispirazione medievale che, unitamente a un nickname in tema, tende a creare un'ambientazione di cavalieri del medio evo. (Wikipedia).

La rivoluzione Google

Internet e Google sembrano oggi un binomio indissolubile: a parte il più famoso motore di ricerca a molti di voi sarà capitato di cercare un itinerario su Google Maps oppure di dare una sbirciatina alle foto del satellite della vostra zona con Google Earth o ancora di produrre e condividere on-line documenti e fogli di calcolo con applicazioni web specifiche e gratuite direttamente on-line con Google Docs. Per il futuro non ci resta che aspettare …

Google Maps

Google Maps è un servizio accessibile dal relativo sito web e che consente la ricerca e la visualizzazione di mappe geografiche di buona parte della Terra. E' anche possibile creare itinerari rispetto a due o più località.

Google Earth

Con *Google Earth* puoi sorvolare tutta la terra e osservare immagini satellitari, mappe, terreno ed edifici 3D.

FIRMA DIGITALE E PROTOCOLLO INFORMATICO

Le istituzioni educative e gli istituti e scuole di ogni ordine e grado hanno l'obbligo di gestire i documenti con sistemi informatici mediante il protocollo elettronico e l'archiviazione elettronica ai sensi del decreto legislativo n. 82 del 7 marzo 2005, il cosiddetto "*Codice dell'amministrazione digitale*".

La precedente Direttiva del Ministro per l'Innovazione e le Tecnologie del 9 dicembre 2002 sulla "*Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali*" evidenziava che l'obiettivo primario di questa innovazione "*è quello di promuovere in tutte le amministrazioni centrali e gli enti pubblici sottoposti alla vigilanza ministeriale la realizzazione di sistemi informativi per la gestione elettronica dei flussi documentali. Ciò allo scopo di assicurare il più rapido e proficuo utilizzo del documento informatico e della firma elettronica negli scambi di documenti ed atti tra amministrazioni, in coerenza con i rispettivi obiettivi istituzionali e con gli obiettivi strategici di digitalizzazione della pubblica amministrazione. Il protocollo informatico e, più in generale, la gestione elettronica dei flussi documentali hanno la finalità di migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei, la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali. Inoltre con tali sistemi ci si prefigge di migliorare la trasparenza dell'azione amministrativa attraverso strumenti che consentano l'accesso allo stato dei procedimenti ed ai relativi documenti da parte di cittadini, imprese ed altre amministrazioni*".

1 La Firma digitale

1.1FIRMA DIGITALE

Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNPIA) precisa che "l*a firma digitale costituisce uno dei cardini del processo di e-governement*[1]*. Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni. Per dotarsi di firma digitale è necessario rivolgersi ai certificatori accreditati: soggetti pubblici e privati che hanno ottenuto l'autorizzazione a svolgere tale attività. L'elenco di tali soggetti è, per legge, pubblicato sul sito del CNIPA. A metà dell'anno 2008 si contano oltre 3,2 milioni di dispositivi di firma digitale."*

1 Per **e-government** (anche **e-gov** o **amministrazione digitale**) si intende il processo di informatizzazione della pubblica amministrazione, il quale - unitamente ad azioni di cambiamento organizzativo - consente di trattare la documentazione e di gestire i procedimenti con sistemi digitali grazie all'uso delle tecnologie dell'informazione e della comunicazione (ICT), allo scopo di ottimizzare il lavoro degli enti e di offrire agli utenti (cittadini ed imprese) sia servizi più rapidi, che nuovi servizi, attraverso - ad esempio - i siti web delle amministrazioni interessate. (Da Wikipedia http://it.wikipedia.org)

L'uso crescente del PC e delle reti telematiche nelle istituzioni scolastiche ha avuto, come conseguenza diretta, la progressiva introduzione di procedure di lavoro compatibili e gestibili dagli **strumenti informatici**.

Un esempio palese di questo fenomeno è stata la necessità di conferire valore giuridico al **documento informatico** e alla **firma digitale**. Infatti, al documento informatico e alla firma digitale è stato attribuito lo stesso valore giuridico del documento sottoscritto con firma autografa. L'aspetto preminente, da non dimenticare, è assicurare l'integrità e la provenienza dei documenti informatici che si *muovono* in un supporto (Internet) tutt'altro che privo di zone d'ombra e soggetto spessissimo ad *attacchi*.

Il CNIPA asserisce che "l'*Italia è posta all'avanguardia nell'uso legale della firma digitale, essendo il primo paese ad avere attribuito piena validità giuridica ai documenti elettronici fin dal lontano 1997 ed essendo quello con maggiore diffusione in Europa."*

FIRMA DIGITALE:
è un procedimento matematico (detto "hash", irreversibile non è possibile, a partire dall'impronta, risalire al documento originario) in grado di produrre su un documento informatico gli stessi effetti giuridici ottenibili tracciando con la penna una firma in calce a un foglio di identità

▽

applicare una firma digitale non vuol dire altro che criptare i documenti in maniera univoca per ogni utente.

PRIMA DI PROCEDERE CON LA TRATTAZIONE A PROPOSITO DELLA FIRMA DIGITALE È BENE CHIARIRE SUBITO CHE…

LA FIRMA DIGITALE NON E' LA RIPRODUZIONE DELLA FIRMA AUTOGRAFA SU UN DOCUMENTO INFORMATICO: NON SI OTTIENE CIOE' TRAMITE IMMAGINI FOTOGRAFICHE O SCANNER

1.2CNIPA E FIRMA DIGITALE

La legge "Bassanini" (Legge 15 marzo 1997, n. 59 - art. 15) e il D.P.R. 10 novembre 1997, n. 513 rendevano validi e rilevanti a tutti gli effetti di legge i documenti informatici, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici.

Il CNIPA (già AIPA) ha assunto un ruolo importante nella predisposizione della normativa del settore. Questa è stata oggetto di varie integrazioni e modifiche e, a oggi, è costituita, tra le altre, dalle seguenti norme:

- Direttiva europea 1999/93/CE sulle firme elettroniche (http://www.giustizia.it/cassazione/leggi/direttiva93_99.html)
- D. Lgs. 7/3/2005, n. 82
- DPCM 13/1/2004
- Deliberazione CNIPA n. 4 del 17/2/2005

- Deliberazione CNIPA n. 34 del 18/1/2006
- Circolare CNIPA n. 48 del 6/9/2005
- CNIPA Linee guida per l'utilizzo della firma digitale.

La firma digitale (che trae valore legale sia dalla L. 59/97 sia dal D.P.R. 513/97) ha trovato l'impianto legislativo necessario per il proprio utilizzo con la pubblicazione, in data 15 aprile 1999, delle regole tecniche costituite dal DPCM 8 febbraio 1999 (oggi sostituito dal DPCM 13 gennaio 2004).

Il D. Lgs. 23 gennaio 2002, n. 10 al comma 3 prescrive che "*il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l' ha sottoscritto*".

Definizioni

Certificato qualificato	Insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Chiave privata	La chiave della coppia utilizzata nel processo di sottoscrizione di un documento informatico
Chiave pubblica	La chiave della coppia utilizzata da chiunque esegua la verifica di una firma digitale
Dispositivo di firma	Insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici
Documento informatico	E' costituito da qualunque oggetto informatico (file) che contenga atti, fatti o dati giuridicamente rilevanti
Firma digitale	E' un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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 autenticazione informatica
Firma elettronica avanzata	Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
Firma elettronica qualificata	La firma elettronica avanzata che sia basata su un certificato qualificato, creata mediante un dispositivo sicuro per la creazione della firma
Soggetto giuridico	Impresa, azienda, società; qualunque soggetto dotato di partita IVA
SSCD	Acronimo inglese (Secure Signature Creation Device) di "dispositivo sicuro per la creazione della firma". E' un dispositivo che soddisfa particolari requisiti di sicurezza. I più utilizzati sono costituiti da smartcard.
Titolare	Il soggetto cui sono attribuite le firme digitali generate attraverso una determinata chiave associata ad un determinato certificato

1.3CHIAVI ASIMMETRICHE

COME FUNZIONA LA FIRMA DIGITALE?

Vista la rilevanza giuridica del documento informatico, occorre poter individuare in maniera semplice colui che l'ha sottoscritto e rilevare subito se il documento è integro oppure è stato in qualche modo alterato dopo la sua sottoscrizione. A tale scopo riveste particolare importanza la *crittografia*, tecnica per rendere intellegibili i documenti a chi non dispone della relativa chiave e dell'algoritmo necessario. La crittografia può essere:

- **simmetrica**, nel caso in cui ogni titolare dispone di una chiave per la firma dei documenti; la stessa chiave dovrà essere in possesso del destinatario che la utilizzerà per la verifica;
- **asimmetrica**, ogni titolare dispone di una coppia di chiavi, una *privata*, mantenuta segreta, che utilizzerà per la sottoscrizione dei documenti, l'altra da rendere *pubblica* che sarà usata per la verifica.

La normativa vigente in Italia, prevede l'uso della *crittografia asimmetrica* per la sottoscrizione dei documenti informatici.

COS' E' UNA COPPIA DI CHIAVI ASIMMETRICHE?

E' una coppia di chiavi *crittografiche*, una privata ed una pubblica, da utilizzarsi per la sottoscrizione dei documenti informatici. Pur essendo univocamente correlate, dalla chiave pubblica non è possibile risalire a quella privata che, come già detto, deve essere custodita in maniera riservata dal Titolare.

- **Chiave privata**: elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico.
- **Chiave pubblica**: 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.

La firma digitale è basata sull'utilizzo di *chiavi*, cioè di veri e propri algoritmi matematici in grado di rendere illeggibili (criptati) documenti informatici, ma riservandone poi la lettura solo a coloro che sono autorizzati .

Ciò vuol dire che ciascuno possiede una propria chiave privata con la quale rende illeggibile un documento (codificare). Solo il possessore della corrispondente chiave pubblica può decodificare il messaggio e viceversa.

1.4LA FUNZIONE DELLA FIRMA DIGITALE

A CHE SERVE LA FIRMA DIGITALE?

La firma digitale è in grado di assolvere a più funzioni, in particolare per la verifica ed il valore e legale di un documento firmato.

PRINCIPALI FUNZIONI DELLA FIRMA DIGITALE

- **RISERVATEZZA**: il documento firmato non deve poter essere compreso da nessun altro se non dal destinatario.
- **INTEGRITÀ**: il documento non deve poter essere modificato da nessuno dopo la firma.
- **AUTENTICAZIONE**: la provenienza del documento deve essere certa.

NON RIPUDIO: chi ha firmato il documento non può negare di averlo fatto (infatti, nessun altro può compilarlo ed emetterlo al suo posto).

Oltre a queste funzioni la firma digitale è in grado di effettuare una certificazione temporale cioè attesta con certezza la data e l'ora della redazione del documento. Infine, per questi motivi, non può ripudiarlo.

QUESTA È UNA CONDIZIONE DETERMINANTE PER LA VALIDITA' LEGALE DI UN DOCUMENTO.

"Esempi tipici dell'utilizzo della firma digitale possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, dichiarazioni di cambi di residenza, di domicilio, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc. Fra privati può trovare un interessante impiego nella sottoscrizione di contratti, verbali di riunioni, ordini di acquisto, risposte a bandi di gara, ecc.

Ancora, la firma digitale trova già da tempo applicazione nel protocollo informatico, nella procedura di archiviazione documentale, nel mandato informatico di pagamento, nei servizi camerali, nelle procedure telematiche d'acquisto, ecc.

Alcuni Comuni che partecipano alla sperimentazione della Carta d'Identità Elettronica hanno dotato i propri cittadini di entrambi gli strumenti (CIE o CNS e Firma Digitale) e sviluppato dei servizi in rete tramite i quali i cittadini possono farsi identificare in rete (CIE/CNS), accedere quindi ai propri dati personali nel pieno rispetto delle norme sulla privacy, e sottoscrivere (firma digitale) dichiarazioni, denunce, ricorsi. Ecco quindi che si intravede l'obiettivo finale: dotarsi di un unico strumento con cui sarà possibile farsi riconoscere e sottoscrivere dichiarazioni, fruendo dei vantaggi derivanti dai servizi in rete". (*Da "Linee guida per l'utilizzo della Firma digitale"*.)

1.5COME CRIPTARE UN DOCUMENTO

Supponiamo di dover spedire un documento che non sia possibile modificare e che il destinatario sia certo per chi lo riceve.

Per prima cosa dobbiamo renderlo illeggibile. Un modo semplice è quello di criptarlo con una chiave specifica. Un esempio di semplice algoritmo consiste nel sostituire le lettere con dei numeri. Quale sarà l'effetto di questa operazione?

Il documento diventerà incomprensibile e solo chi conosce il criterio di sostituzione (ovvero possiede la chiave) è in grado di leggerlo

Per la firma elettronica ogni titolare di firma ha un meccanismo di criptazione *unico*, formato da migliaia di regole non ricostruibili in alcun modo. Solo avendo la chiave di criptazione è possibile riottenere il documento originario.

I sistemi a chiave singola non possono essere usati come sistemi a validità legale in quanto richiedono la diffusione ai mittenti della chiave personale dell'utente e quindi un rischio inaccettabile di utilizzo improprio.

Per questo motivo, come è già stato detto, vengono utilizzate le chiavi asimmetriche (una *pubblica* e una *privata*) rilasciate da autorità di certificazione che hanno il compito di assegnare univocamente una chiave (firma) ad una persona specifica.

1.6COME USARE LA FIRMA DIGITALE

Supponiamo che la scuola "Alfa" debba inviare un documento alla scuola "Gamma". E' ovvio che quest'ultima ha la necessità di sapere,senza possibilità di dubbio, che:

- il documento è stato effettivamente spedito dalla Scuola "Alfa";
- il documento non è stato modificato dopo l'invio;
- la scuola "Alfa" non abbia possibilità di ripudiarlo (cioè non riconoscerlo come suo).

I PASSI DA COMPIERE POSSONO ESSERE SEMPLIFICATI COME SEGUE:

1. La scuola "Alfa" firma il documento con la propria chiave privata rendendolo illeggibile e lo invia alla Scuola "Gamma" allegando anche una copia del proprio certificato digitale che contiene i dati del certificatore, il nome di "Alfa" e la chiave pubblica;
2. la scuola "Gamma" prende il documento, si procura la chiave pubblica della scuola "Alfa" per verificare l'autenticità della firma.

Se la chiave pubblica utilizzata dalla Scuola "Gamma" è identica a quella contenuta nel certificato digitale il documento sarà **sicuramente** stato spedito dalla Scuola "Alfa".

NATURALMENTE QUESTO SISTEMA SI BASA SULLA SICUREZZA (NON MODIFICABILITA' E NON ACCESSO) DEL CERTIFICATO DIGITALE CHE VIENE FIRMATO CON LA CHIAVE PRIVATA DEL CERTIFICATORE.

In questo modo sono garantiti:

- **Inalterabilità**
  Gli stessi algoritmi consentono di verificare se al documento sono state apportate modifiche dopo l'invio (nella firma digitale è contenuta un'immagine di quel determinato documento).
- **Non ripudio**
  Solo la scuola "Alfa" possiede la chiave privata; pertanto solo la scuola "Alfa" era in grado di "generare la propria firma".
- **Identità del firmatario**

L'identità del firmatario è assicurata da un certificato digitale che ha lo scopo proprio di garantire la corrispondenza tra chiave pubblica e privata e una determinata persona giuridica (o fisica). In altre parole è necessario che una terza parte neutra (una autorità di certificazione autorizzata) garantisca che quella firma è proprio della scuola "Alfa".

Per garantire l'identità dei soggetti che utilizzano la firma digitale e per fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, il DPR n. 513/97 (art. 8) richiede che il soggetto certificatore sia in possesso di particolari requisiti e sia incluso in un elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura del CNIPA che svolge attività di sorveglianza.

Le Pubbliche Amministrazioni possono anch'esse certificare le chiavi osservando le regole tecniche dettate dalla normativa in vigore: possono richiedere di essere accreditate (iscritte quindi nell'elenco pubblico dei certificatori) utilizzando in realtà le infrastrutture tecnologiche di uno dei soggetti già iscritti nell'elenco pubblico dei certificatori. In questo caso ottengono il vantaggio di risultare, nella fase di verifica di un documento informatico sottoscritto con firma digitale da un proprio dipendente, quali soggetti che emettono e garantiscono le informazioni inerenti il dipendente stesso.

Dove e come dotarsi di firma digitale

"Coloro che intendono dotarsi di quanto necessario per poter sottoscrivere con firma digitale documenti informatici possono rivolgersi ad uno dei soggetti autorizzati: i **Certificatori**.

L'elenco pubblico dei certificatori è disponibile via Internet per la consultazione, dove sono anche disponibili i link ai siti web degli stessi sui quali sono indicate le modalità operative da seguire. E' bene precisare che vi sono alcuni soggetti che espletano questa attività esclusivamente per gruppi chiusi di utenti.

E' il caso del Centro Tecnico che esercita l'attività di certificatore esclusivamente per le PA appartenenti alla Rete Unitaria della Pubblica Amministrazione, piuttosto che l'Esercito Italiano o il Consiglio Nazionale del Notariato, che svolgono detta attività solo per gli appartenenti alle proprie strutture.

Esclusi questi soggetti vi sono, ad oggi, circa una ventina di certificatori accreditati cui rivolgersi.

Il kit di firma digitale ed i costi

Per poter generare firme digitali è necessario essere dotati di un dispositivo sicuro per la generazione delle firme (costituito da una smartcard o da un token USB), un lettore di smartcard (nel caso in cui non si utilizzi il token USB), un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso (es. per il cambio del PIN che ne consente l'uso).

I costi del kit completo sono variabili da certificatore a certificatore. Il CNIPA (da cui sono state estratte queste informazioni) informa a mero titolo esemplificativo che è possibile ottenere il kit completo ad un prezzo di circa 100 €. Il certificato ha una scadenza, e deve essere quindi rinnovato periodicamente. In genere hanno una validità di uno o due anni, il rinnovo ha un costo orientativo di 10/15 € per anno. E' bene evidenziare che tutti i certificatori prevedono delle condizioni economiche specifiche per forniture di particolare rilievo.

1.7IMPORTANZA DELLA FIRMA DIGITALE

LA GRANDE IMPORTANZA DELLA FIRMA DIGITALE CONSISTE NEL FATTO CHE L'AUTENTICITA' DEI DOCUMENTI NON VIENE VERIFICATA TRAMITE "PERIPEZIE" CALLIGRAFICHE COME AVVIENE PER I DOCUMENTI NORMALI

MA

CON STRUMENTI E FORMULE MATEMATICHE CHE ASSICURANO L'IMPOSSIBILITA' DI IMITARE, FALSIFICARE O MODIFICARE LA FIRMA SU UN DOCUMENTO.

NATURALMENTE CIO' COMPORTA LA NECESSITA' DI UNA GRANDE EVOLUZIONE CULTURALE E DI PENSIERO E UNA CONSUETUDINE ALL'USO DI STRUMENTI INFORMATICI IN LINEA CON LE POLITICHE DI MODERNIZZAZIONE ED EVOLUZIONE ORGANIZZATIVA DELLA P.A. IN ITALIA NEGLI ULTIMI ANNI.

1.8USI DELLA FIRMA

LA FIRMA ELETTRONICA CONSENTE IL FLUSSO TELEMATICO DI DOCUMENTI IN FORMATO ELETTRONICO CHE ACQUISISCONO CONSEGUENTEMENTE **VALIDITA' LEGALE**

CONDIZIONE ESSENZIALE PER EVITARE FALSIFICAZIONI DI FIRMA È CHE IL TITOLARE DELLA COPPIA DI CHIAVI MANTENGA RISERVATA LA PROPRIA CHIAVE PRIVATA.

A tal proposito, le norme tecniche prescrivono che:

1. le chiavi private sia conservate e custodite all'interno di un dispositivo di firma. È possibile utilizzare lo stesso dispositivo per conservare più chiavi;
2. è vietata la duplicazione della chiave privata o dei dispositivi che la contengono;
3. per fini particolari di sicurezza, sia consentita la suddivisione della chiave privata su più dispositivi di firma.

La chiave privata, eventualmente registrata su supporti magnetici, potrà anche servire per accertare l'identità di un utente che deve accedere a servizi che richiedono l'identificazione (rilascio di certificati, l'uso di servizi a pagamento, l'accesso ad informazioni personali, ecc…)

A proposito della riservatezza delle chiavi la normativa prevede che Il titolare delle chiavi debba:

- conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;

- richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia
- perduto il possesso o risultino difettosi.

Come si firma un documento

"La firma digitale di un documento dipende dal software di firma di cui si dispone. Tale software, come già detto, può essere fornito da un certificatore, ma sono disponibili anche numerosi prodotti sviluppati da altre aziende. Indipendentemente dal prodotto però i passi per la sottoscrizione digitale di un singolo documento sono sempre gli stessi. Vediamo quali.

Ovviamente bisogna disporre di un personal computer al quale preventivamente abbiamo collegato il lettore/scrittore di smart card in base alle indicazioni del fornitore.

Dopo averlo attivato il software di firma ci richiederà di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore se ancora non lo si è fatto. All'attivazione del processo di firma ci verrà richiesto di inserire il codice PIN della smart card e dopo qualche secondo potremo salvare un file sottoscritto e pronto per essere utilizzato.

E' importante ricordare che in base alla legislazione vigente sull'interoperabilità della firma digitale il file sottoscritto conserva il suo nome originale, al quale viene aggiunta l'estensione ".p7m". Ne risulta che, ad esempio, il file mensa.pdf, dopo la sottoscrizione, diverrà mensa.pdf.p7m e come tale sarà fruito da altre applicazioni.

Per completezza d'informazione la procedura di firma digitale può essere effettuata anche attraverso procedure automatiche, purché ci si attenga a particolari cautele indicate anche dalla legislazione vigente."

Come si verifica un documento

"La procedura di verifica della firma digitale apposta ad un documento informatico consiste sostanzialmente nel verificare che:

- il documento non sia stato modificato dopo la firma;
- il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
- il certificato del sottoscrittore non sia scaduto;
- il certificato del sottoscrittore non sia stato sospeso o revocato.

Per eseguire queste verifiche, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software. Detti software sono forniti dai certificatori ai titolari dei certificati; coloro che non sono dotati di un kit di firma digitale possono altresì utilizzare dei software disponibili per uso personale a titolo gratuito: attualmente ne sono stati segnalati quattro, tre da installare sul proprio PC, il quarto disponibile via web. Detti software freeware sono stati resi disponibili dal CNIPA (Verifica_CT – www.cnipa.gov.it/), dalla Comped (DigitalSign – www.comped.it/), da Postecom (FirmaOK – www.poste.it/online/postecert), dalla società Digitaltrust (Sign'ncrypt – www.signncrypt.it) e da TrustItalia (Signo Reader – https://firmadigitale.trustitalia.it/). Per eseguire la verifica non è necessario

disporre di smartcard e lettore, in sintesi non si deve essere necessariamente dotati del kit di firma digitale.

Per eseguire le verifiche di cui ai punti 1, 2 e 3 è sufficiente essere dotati di un personal computer, di un prodotto utile per la verifica, piuttosto che del collegamento ad Internet per la verifica con il prodotto disponibile via web. Per la verifica al punto 4 è necessario avere accesso ad Internet. Difatti, i software di verifica si collegano alla lista di revoca dove il certificatore che ha emesso il certificato qualificato renderà disponibili le informazioni relative alla sospensione o revoca del certificato nel caso in cui si verifichi.

Per la verifica al punto 2 è necessario che sui software installati sul client siano stati caricati i certificati di certificazione dei soggetti iscritti nell'elenco pubblico."

1.9Firme "leggere" e firme "forti"

Comunemente si sente parlare di firma "leggera" e di firma "forte". Queste definizioni sono state introdotte dagli addetti ai lavori per sopperire alla mancanza di una definizione esplicita di altre tipologie di firma.

Questa distinzione è stata introdotta per distinguere una firma più importante dal punto di vista legale perché equivalente alla sottoscrizione autografa. Spesso, appunto, ci si riferisce ad essa con il termine firma "forte". Essa soddisfa specifiche caratteristiche derivanti dal certificatore. Deve essere apposta con strumenti sicuri come ad esempio un smart card.

Riassumendo, affinché la firma apposta possa essere considerata equivalente ad una autografa:

a) deve essere basata su un sistema a chiavi asimmetriche;
b) deve essere generata con chiavi certificate con le modalità previste nell'allegato I della Direttiva
c) deve essere riconducibile a un sistema di chiavi provenienti da un certificatore operante secondo l'allegato II della Direttiva Europea del 1999 e soggetto a vigilanza da parte di un organo definito (il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri);
d) deve essere generata utilizzando un dispositivo sicuro che soddisfi i requisiti dell'allegato III della stessa Direttiva.

Il secondo comma dell'articolo 5 della Direttiva conferisce dignità giuridica alle altre tipologie di firma. Esse non sono definibili tecnologicamente a priori. Possono essere generate senza vincoli sugli strumenti e sulla modalità operative. E' ovvio che non offrono garanzie di interoperabilità se non in particolari condizioni di utilizzo come in gruppi chiusi di utenti. Infatti, in questo caso, la comunità di utenti condivide gli strumenti di firma e di verifica della stessa. Un giudice, non potrà rifiutare in giudizio queste firme "leggere", ma la loro ammissibilità nascerà dalla libera convinzione e non dall'obbligo di legge previsto per le firme cosiddette "forti".

1.10FIRMA DIGITALE E P.A.

PUO' NON RISULTARE SUPERFLUO RIPETERE ALCUNI CONCETTI PRINCIPALI:

- La firma digitale trasforma una sequenza del bit, fino a prima della sua introduzione, privi di rilevanza giuridica in un vero e proprio documento informatico a cui la normativa italiana, sotto precise condizioni attribuisce la stessa validità del documento su supporto cartaceo.
- La Legge Bassanini (Legge 15 marzo 1997, n. 59 – art. 15) e il DPR 10 novembre 1997, n. 513 rendono validi e rilevanti a tutti gli effetti di legge i documenti informatici, la loro archiviazione su supporto informatico e la trasmissione con strumenti telematici.
- Diventa perciò una realtà per le Pubbliche Amministrazioni, le imprese ed i privati scambiare documenti elettronici con la stessa validità dei corrispondenti documenti cartacei.

Va detto che l'uso legale della firma digitale porterà enormi benefici sia per il settore pubblico che per quello privato, perché migliorerà i processi della Pubblica Amministrazione mediante la razionalizzazione, semplificazione ed accelerazione dei provvedimenti amministrativi.

VERSO UN SISTEMA INFORMATICO DELLA P.A.

1.Il sistema informativo della P.I.

1.1CAMBIAMENTO ORGANIZZATIVO

Per fare fronte alle esigenze di comunicazione, efficienza ed efficacia nei servizi delle scuole ed dell'intera struttura tecnica che fa capo al MIUR e non solo, si rende necessaria la progettazione di un nuovo modello organizzativo, l'acquisizione di nuove competenze professionali e la rielaborazione della cultura preesistente attraverso la riformulazione degli obiettivi strategici dell'organizzazione a fronte di nuove esigenze di mercato.

EVOLUZIONE MERCATO:
- Più efficace governo della cosa pubblica
- Migliore qualità dei servizi
- Integrazione Europea

NUOVE STRATEGIE
DA: SUPPORTO
A: OFFERTA

EVOLUZIONE ORGANIZZATIVA STRUTTURALE CULTURALE
- S.I.D.
- S.F.

SIDI - Sistema Informativo Dell'Istruzione

SPC - Sistema Pubblico di Connettività

1. Il processo di trasformazione di una struttura organizzativa è sollecitato ogni qualvolta evolve il contesto socio-economico ove si colloca la sua attività lavorativa.
2. La nuova realtà di mercato rende imprescindibile, pena l'emarginazione dal contesto socio-economico, l'avvio del

processo di adattamento della struttura mediante un insieme di interventi sia a livello strategico, che strutturale e culturale.

In particolare nella P.I., sulla base dei nuovi orientamenti e sviluppi della scuola nasce, per esempio, la necessità di garantire, in un contesto organico ed integrato, la pianificazione dei fenomeni scolastici quale strumento di supporto alla politica della scuola ed al suo governo, attraverso la gestione e la conoscenza dei fenomeni stessi.

L'evoluzione del mercato e dell'economia richiede sempre di più una nuova fisionomia dei servizi amministrativi, questo implica il superamento del tradizionale ruolo di supporto al funzionamento delle Istituzioni Pubbliche a favore di un ruolo di offerta di un servizio di qualità al cittadino.

Una tale evoluzione implica non solo la progettazione di un nuovo modello organizzativo, ma anche l'acquisizione di nuove competenze professionali e la rielaborazione della cultura preesistente con la riformulazione degli obiettivi strategici dell'organizzazione a fronte di nuove esigenze di mercato.

1.2TECNOLOGIE INFORMATICHE ED AUMENTO DI EFFICIENZA

TECNOLOGIE INFORMATICHE

Con il termine TIC si intendono le Tecnologie della Comunicazione e dell'Informazione ovvero le ICT (Information and Communication Tecnology)

Riorganizzazione dell'intero processo lavorativo

Incremento ll'efficienza complessiva dei processi e dei servizi

Evoluzione organizzativa e strutturale

IL PROGETTO DI TRASFORMAZIONE DEL SISTEMA INFORMATIVO DEL MINISTERO DELLA PUBBLICA ISTRUZIONE, DA CENTRALIZZATO A DECENTRATO, RAPPRESENTA LA RISPOSTA PIU' APPROPRIATA ALLE ESIGENZE DELL'AMMINISTRAZIONE VOLTE AL RAGGIUNGIMENTO DI TALI OBIETTIVI.

Le tecnologie informatiche possono essere utilizzate per realizzare in maniere efficiente il funzionamento organizzativo previsto dal nuovo modello.

In tal senso, lo sviluppo di un Sistema Informativo è finalizzato alla innovazione del processo organizzativo della struttura in evoluzione.

Tuttavia, come abbiamo già detto, l'attuazione di un nuovo modello organizzativo richiede l'attivazione di un processo soggettivo e collettivo di acquisizione di competenze ed elaborazione della cultura acquisita, che rende imprescindibile il coinvolgimento della risorsa umana.

Dopo una prima fase, in cui le tecnologie informatiche hanno ricoperto un ruolo fondamentale di miglioramento dell'efficienza gestionale delle singole attività del servizio a fronte delle nuove esigenze emerse, in Pubblica istruzione si è passati ad una fase innovativa, in cui l'impiego delle tecnologie è finalizzato

alla *riorganizzazione dell'intero processo lavorativo del servizio*, in modo da potenziarne l'efficienza.

NELLA PUBBLICA ISTRUZIONE, QUINDI, LE TECNOLOGIE INFORMATICHE ASSUMONO IL RUOLO DI INNOVAZIONE DELL'ORGANIZZAZIONE DEL SERVIZIO, CHE RISULTA IMPRESCINDIBILE DAL RAGGIUNGIMENTO DELL'OBIETTIVO STRATEGICO FINALE DI MIGLIORARE LA QUALITÀ DELL'OFFERTA DEL SERVIZIO AL CITTADINO.

1.3IL VECCHIO SISTEMA INFORMATIVO

1975 NASCE IL PRIMO SISTEMA INFORMATIVO DELLA PUBBLICA ISTRUZIONE

I suoi due principali obiettivi erano:

- la gestione automatica delle aree operative attinenti agli 'organici', al 'movimento' ed al 'reclutamento' del personale scolastico;
- lo studio e la graduale estensione dei processi di automazione ad altri settori operativi comprendenti la gestione contabile (contabilità speciale) e giuridica (ricostruzione delle carriere, riscatti, stato matricolare…) del personale della scuola, oltre che settori diversi dell'attività amministrativa degli Uffici Centrali e Periferici della P.I.

Nel 1975:

- l'aumento della popolazione scolastica, dovuta sia all'istituzione della scuola materna statale, sia ad un aumento delle iscrizioni alle scuole medie superiori conseguente all'incremento demografico del dopoguerra;
- la considerazione dell'entità numerica del personale amministrativo (oltre un milione di persone: la più grande azienda del Paese);
- le profonde innovazioni normative (per esempio, leggi speciali per il reclutamento, conseguenti al boom demografico);
- la complessità del servizio scolastico;
- le sempre più urgenti esigenze di conoscenza, valutazione e controllo delle innumerevoli variabili del fenomeno scolastico;

e quindi la complessità gestionale derivante…..

RENDEVA NECESSARIO INTRODURRE UNO STRUMENTO DI GESTIONE INFORMATICO CAPACE DI PREVENIRE ED EVITARE LA PARALISI DEI NODI FONDAMENTALI DELL'ORGANIZZAZIONE (GLI UFFICI CENTRALI E LE SEDI PERIFERICHE).

1.4LE NUOVE ESIGENZE

NEL CORSO DEGLI ANNI IL SISTEMA INFORMATIVO RAGGIUNSE I SUOI OBIETTIVI

MA….

NUOVE ESIGENZE DI INFORMATIZZAZIONE EMERSERO SIA DAGLI

UFFICI CENTRALI E PERIFERICI DELL'AMMINISTRAZIONE, SIA DALLE UNITA' SCOLASTICHE, PERCIO' SI INIZIO' A PENSARE AD UN NUOVO SISTEMA!

1. Gli obiettivi che si era posto il primo Sistema Informativo sono stati raggiunti, ma nel corso degli anni successivi allo sviluppo, sono emerse nuove esigenze di informatizzazione provenienti sia dagli Uffici Centrali e Periferici dell'Amministrazione sia dalle unità scolastiche, strutture erogatrici del servizio fornito dal Sistema Scolastico Nazionale.
2. Categorie e concetti quali "concorrenza" e "competitività" si stanno affermando finalmente anche nella Pubblica Amministrazione e sono imposti non solo dal processo di integrazione europea, ma soprattutto, dalla domanda, sempre crescente da parte dei cittadini, di una migliore qualità dei servizi e di un migliore governo della cosa pubblica.
3. Le lamentele per i "disservizi" e per gli insuccessi registrati si fanno sempre più incalzanti, non tanto per un degrado della Pubblica Amministrazione, quanto per una crescente maturità dei cittadini che si sono fatti sempre più esigenti.

1.5DAL CENTRALISMO AL DECENTRAMENTO

Negli anni 80 si avvertì l'esigenza di evolvere il sistema informativo e di rendere sempre più decentralizzato includendo le scuole nel processo di nuova informatizzazione

IN PARTICOLARE PER:

- migliorare il servizio
- ridurre la complessità gestionale del sistema
- disporre di una base di dati che garantisca adattabilità del sistema informatico alle particolarità locali

Si affermarono quindi improrogabili esigenze di snellimento, unificazione e semplificazione delle attività organizzative interne degli uffici.

1. In questa fase, l'amministrazione scolastica è matura per un profondo rinnovamento strutturale di vasta portata, che ha reso necessaria la ricerca di nuove forme di architettura del suo Sistema Informativo e ha fatto nascere improrogabili esigenze di snellimento, unificazione e

semplificazione delle attività organizzative interne degli uffici, raccordate con problematiche di gestione proprie del Sistema.

2. D'altra parte, la necessità di agevolare il reperimento e la gestione dei dati hanno reso indispensabile un nuovo disegno funzionale del Sistema Informativo, secondo criteri di integrazione e storicizzazione dei dati gestiti.

1.6VANTAGGI NELL'UTILIZZO DI UN SISTEMA INFORMATIVO

MA QUALI SONO I VANTAGGI DI UN SISTEMA INFORMATIVO PER LA P.I.?

Le tecnologie informatiche furono utilizzate per realizzare un sistema informativo che innovasse il processo organizzativo mediante:

DECENTRAMENTO permette di svolgere direttamente presso i siti interessati le elaborazioni di pertinenza	INTEGRAZIONE riduce il lavoro di validazione dell'informazione da parte dei funzionari amministrativi al solo momento di ingresso del dato nel Sistema Informativo

Il nuovo Sistema Informativo consente infatti di realizzare una più efficiente organizzazione del servizio mediante il decentramento delle applicazioni gestionali e l'integrazione di esse al fine di garantire continuità al servizio in termini di sicurezza e coerenza dei dati:

LA GESTIONE NON È PIU' DEL DATO MA DELL'INTERO PROCESSO!

L'INNOVAZIONE DEL PROCESSO ORGANIZZATIVO

DECENTRAMENTO E INTEGRAZIONE DELLE APPLICAZIONI	**SID**

GESTIONE NON PIU' DEL DATO MA DELL'INTERO PROCESSO

- **MAGGIORE RISPETTO DELLE SCADENZE**
- **MAGGIORE PRODUTTIVITA'**
- **MAGGIORE QUALITA' DEL SERVIZIO OFFERTO.**

Le tecnologie informatiche sono state utilizzate per lo sviluppo di un sistema informativo che consente l'innovazione del processo organizzativo mediante:

- il **DECENTRAMENTO**, un'architettura distribuita su tutto il territorio nazionale per consentire il maggior decentramento possibile delle applicazioni gestionali, permettendo di svolgere direttamente presso i siti interessati le elaborazioni di pertinenza; tali elaborazioni opereranno in aggiornamento esclusivamente sui dati di loro

proprietà. Grazie al decentramento, ad esempio, circa l'80% degli uffici riuscirà ad espletare tutti gli adempimenti amministrativi relativi all'organico di diritto entro le date in cui, generalmente, si concludono le sole operazioni di movimento. Gli uffici di grandi dimensioni saranno in grado di accelerare notevolmente i tempi di svolgimento degli adempimenti di organico di diritto e, di conseguenza, si potranno anticipare le operazioni relative all'organico di fatto, per garantire un corretto avvio dell'anno scolastico, in accordo con le date di effettivo inizio delle lezioni.

- **l'INTEGRAZIONE**, una gestione integrata delle informazioni trattate dalle diverse procedure amministrative, in modo da ridurre il lavoro di validazione dell'informazione da parte dei funzionari amministrativi al solo momento di ingresso del dato nel Sistema Informativo.

Il Sistema **I**nformativo **D**ecentrato, consente infatti di realizzare una più efficiente organizzazione del servizio mediante il decentramento delle applicazioni gestionali e l'integrazione di esse al fine di garantire continuità al servizio in termini di sicurezza e coerenza dei dati.

IL DATO ORA SI ATTINGE UNA VOLTA SOLA DOVE SI GENERA E VIENE DECENTRATO CAPILLARMENTE PER ESSERE UTILIZZATO LÀ DOVE SERVE, MEDIANTE LA REALIZZAZIONE DI UNA UNICA BASE DATI PER TUTTE LE PROCEDURE DEL SISTEMA.

IN TAL MODO IL NUOVO SISTEMA INFORMATIVO CONSENTE DI GESTIRE IN MANIERA EFFICIENTE NON IL SINGOLO DATO MA L'INTERO PROCESSO LAVORATIVO AUMENTANDONE LA VISIBILITÀ E LA COERENZA INTERNA.

La trasparenza dell'intero processo lavorativo, individuando le interdipendenze funzionali, consente un maggior controllo sulle scadenze intermedie e garantisce contemporaneamente un maggior rispetto globale delle scadenze finali.

La coerenza interna al processo lavorativo, determinata dalla distribuzione del carico di lavoro e l'eliminazione delle ridondanze, garantisce una maggiore produttività.

1.7I LIVELLI DI UTENZA

L'architettura del nuovo Sistema Informativo si sviluppa su tre livelli di utenza:

1. Uffici Centrali – Un Sistema di Governo, Controllo e Misura delle performance alimentato con i dati delle procedure operative e arricchite con fonti esterne (ISTAT, MEF, INPDAP, ecc,)
2. Uffici Scolastici Regionali
3. Istituzioni Scolastiche.

Ciascuno di essi possiede sistemi di elaborazione, funzioni automatiche e organizzazione dimensionati in base alle specifiche esigenze del livello ed è collegato in rete con tutti gli altri.

NEL SISTEMA ASSUMONO UN RUOLO CENTRALE LE ISTITUZIONI SCOLASTICHE. CIO' ESPRESSO DAL FATTO CHE COSTITUISCONO:

- punto di origine della domanda di servizio nei confronti dell'amministrazione (attività di acquisizione);
- punto terminale di erogazione del servizio ai diversi utenti: alunni, genitori, operatori scolastici ("attività di erogazione").

Approfondimento…

L'architettura del nuovo Sistema Informativo Decentrato si sviluppa su tre livelli di utenza:

- Uffici Centrali
- Uffici Scolastici Regionali
- Scuole.

Ogni livello possiede sistemi di elaborazione, funzioni automatiche e organizzazione, dimensionati in base alle specifiche esigenze del livello.

Ciascun livello può:

- utilizzare le funzionalità in "locale", se disconnesso dalla rete;
- operare, connesso in rete, per scambiare con gli altri livelli i dati elaborati localmente.

Il sistema centrale svolge funzioni di monitoraggio e gestione della rete informativa.

Il piano operativo prevede l'estensione graduale del decentramento, fino a coprire tutte le Istituzioni Scolastiche presenti sul territorio nazionale, sedi di presidenza e circoli didattici.

Forniamo un quadro riassuntivo delle funzionalità offerte dal S.I.D. prima di entrare nel merito delle attività caratteristiche delle Istituzioni Scolastiche.

"Ci soffermeremo, in particolare, sulle Istituzioni Scolastiche che, va sottolineato, assumono un ruolo centrale nel contesto del nuovo Sistema informativo".

La centralità del ruolo delle Istituzioni Scolastiche è espressa dal fatto che esse costituiscono:

- punto di origine della domanda di servizio nei confronti dell'amministrazione (attività di acquisizione);
- punto terminale di erogazione del servizio ai diversi utenti: alunni, genitori, operatori scolastici (attività di "erogazione").
- L'entità scuola è considerata come "unità organizzativa autonoma", in quanto punto di snodo tra le attività di:
- programmazione e controllo proprie del Capo d'Istituto e degli Organi Collegiali.
- erogazione ed amministrazione del servizio scolastico.

A tal fine il Sistema Informativo garantisce anche la disponibilità di efficaci strumenti di ausilio per le attività svolte all'interno delle Istituzioni Scolastiche: gestione degli alunni, predisposizione di strumenti e sussidi didattici, gestione del personale, gestione finanziaria e patrimoniale, attività di pianificazione, controllo e governo, attività di ufficio.

Le segreterie delle scuole diventano lo sportello automatico di quasi tutte le attività di acquisizione, controllo e validazione dei dati, garantendo la correttezza e l'unicità del dato.

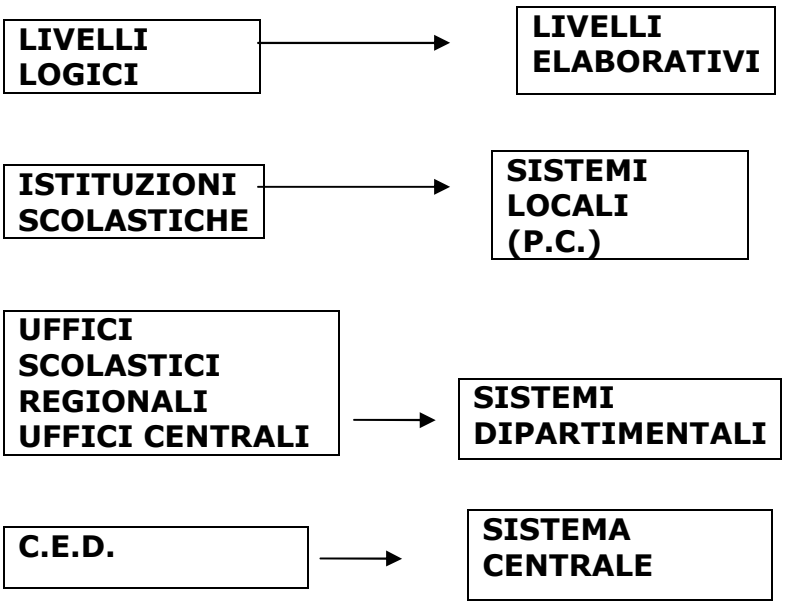
Inoltre, mediante l'utilizzo delle funzioni del S.I.D., i Capi d'Istituto traggono beneficio operativo ed economico. Infatti, le Istituzioni Scolastiche di ogni ordine e grado, hanno recentemente ottenuto una maggiore autonomia gestionale rispetto alla Direzione Regionale, spesso, però, senza avere adeguate conoscenze per utilizzarla in maniera opportuna. L'utilizzo delle funzioni del S.I.D., invece, permette comunque al personale delle Segreterie Scolastiche di adempiere a tutti i procedimenti previsti nelle aree riguardanti la gestione del bilancio e il pagamento degli stipendi.

Ad esempio, risulta facilitato il pagamento delle supplenze brevi anche nelle Scuole Primarie, mentre, precedentemente, questa operazione era completamente a carico della Direzione Regionale competente, con ovvii disservizi di ritardo e aggravi di lavoro per la Direzione Regionale stessa. Da ciò si deduce che il nuovo S.I.D. rappresenta per l'utilizzatore un indispensabile supporto procedurale in occasione della stesura del bilancio, contabile per il pagamento degli stipendi, giuridico per la ricostruzione delle carriere.

1.8INDIVIDUAZIONE DEI LIVELLI LOGICO-TERRITORIALI

IL NUOVO SISTEMA INFORMATIVO PREVEDE:

- Sistemi locali, dislocati presso le scuole;
- Sistemi Dipartimentali, dislocati presso gli Uffici centrali e Periferici del Ministero (Uffici Scolastici Regionali Uffici Centrali);
- Sistema Centrale, localizzato presso il centro Elaborazione Dati di Monteporzio Catone.



L'individuazione dei tre livelli (territoriali) di utenza, con le attività di loro competenza, ha consentito altresì di associarvi, in termini di "sistema di elaborazione dati", tre livelli elaborativi:

- *Locale*, nel quale vengono trattate le informazioni di proprietà di ciascuna Istituzione Scolastica;
- *Dipartimentale*, dove sono gestite le funzioni che richiedono l'utilizzo delle informazioni di proprietà di ciascuna Direzione Regionale. CSA o Ufficio Centrale;
- *Centrale*, in cui vengono svolte le funzioni che richiedono l'utilizzo dei dati riguardanti l'intero Sistema Informativo.

L'architettura, pertanto, è di tipo decentrato, con potenza elaborativa e base informativa decentrate (logicamente e fisicamente) secondo precisi criteri di aggregazione.

Per la sua realizzazione è stato necessario identificare apparecchiature in grado di soddisfare le necessità elaborative di ciascun livello logico individuato e stabilire le interazioni tra essi, al fine di consentire il corretto flusso elaborativo delle applicazioni. I principali elementi, che costituiscono questa architettura vengono classificati come segue:

- *Sistemi Locali*, dislocati presso le scuole;
- *Sistemi Dipartimentali*, dislocati presso gli Uffici Centrali e Periferici del Ministero (Uffici Scolastici Regionali, Uffici Centrali);
- *Sistema Centrale*, localizzato presso il Centro Elaborazione Dati di Monteporzio Catone.

1.9RETE PRIVATA DI COLLEGAMENTO

CENTRO ELABORAZIONE DATI (C.E.D.)
(Monteporzio Catone RM)

Ministero della Pubblica Istruzione

Direzione Regionali

Uffici periferici del M.P.I.

La configurazione prevede il collegamento del Sistema centrale, ubicato a Monteporzio, con l'Ufficio Periferico mediante circuiti diretti numerici ad alta velocità mentre le stazioni di lavoro dislocate negli uffici, i server di comunicazione e il server di rete, costituito da un sistema Unix dimensionato secondo le esigenze locali, compongono la rete locale degli Uffici Periferici del M.P.I.

La rete privata esistente permette il collegamento delle Direzioni Regionali e degli Uffici Centrali del Ministero della Pubblica Istruzione con il Centro Elaborazione Dati (C.E.D.) sito a Monteporzio Catone.

Tale rete è costituita da una struttura primaria di configurazione punto-punto tra il C.E.D. e i punti di concentrazione distribuiti sul territorio nazionale; da questa struttura primaria avente topologia stellare, si dirama una struttura

secondaria in configurazione punto-punto e/o multipunto, che collega ogni punto di concentrazione con gli uffici periferici ad esso più vicini, tramite almeno due linee.

1.10ARCHITETTURA DELLE DIREZIONI REGIONALI e DEI CSA

L'ORGANIZZAZIONE DEL SERVIZIO
LA RETE DI TRASMISSIONE DATI

RETE LOCALE DELLA DIREZIONE REGIONALE

C.E.D. MONTEPORZIO CATONE

RETE TELEMATICA

UFFICI SCUOLE

L'architettura per le Direzioni Regionali prevede nel sistema informativo attuale:

1. sistema dipartimentale
2. posti di lavoro
3. elaboratori di comunicazione
4. stampanti gestionali in rete locale.

SI DEVE COMUNQUE TENERE PRESENTE CHE:

L'EVOLUZIONE NORMATIVA ED ORGANIZZATIVA DEL MINISTERO DELLA P.I, SICURAMENTE NEL FUTURO MODIFICHERA' ANCORA L'ARCHITETTURA DEL SISTEMA INFORMATIVO SOPRATTUTTO PER CIO' CHE RIGUARDA LE DIREZIONI REGIONALI, I CSA, e LE ISTITUZIONI SCOLASTICHE

Sistema Dipartimentale

Il dipartimentale è dotato di sistema operativo di tipo UNIX.

Le risorse del sistema (memoria centrale, memoria di massa, dispositivi di comunicazione, stampanti...) sono dimensionate in base al carico previsto e dipendenti dall'utenza da servire.

Per effettuare il salvataggio della base dati locale, si dispone di un'unità a cartuccia.

Per garantire un corretto funzionamento del sistema si utilizzeranno mini gruppi di continuità o batterie tampone, che consentono una corretta chiusura del sistema a fronte di interruzione di corrente.

1.11I POSTAZIONI DI LAVORO

- Sono costituiti da personal computer dotati di stampante laser o a getto d'inchiostro, da cui svolgere funzionalità di informatica

individuale (elaborazione testi Microsoft Word, Foglio Elettronico Excel) di automazione d'ufficio (Protocollo, Archivio, Processi Amministrativi)
• Inoltre consentono ai posti di lavoro l'accesso alla rete privata permettendo così il colloquio con il sistema centrale di Monteporzio Catone e con le Istituzioni scolastiche.

Le vecchie PDL (Posti di Lavoro o Postazioni Di Lavoro) erano (o sono ancora in pochissimi sporadici casi) differenziate su tre diverse tipologie: *Tipo 1,Tipo 2 Tipo 3* a seconda del livello di utenze e accesso al sistema informativo centrale ed erano dotate di sistema operativo *Windows 95 ormai sparito dalla circolazione.*

Negli ultimi tre anni le vecchie PDL (Posti di Lavoro o Postazioni Di Lavoro) sono state sostituite dai più moderni PC a disposizione delle singole Istituzioni Scolastiche autonome, in particolare le linee trasmissive del sistema di comunicazione sono state trasformate e sono state dismesse le vecchie linee ISDN con le più veloci e funzionali linee ADSL

La posta elettronica del Sistema Informativo del Ministero della Pubblica Istruzione mette a disposizione una serie di funzionalità; da una qualsiasi postazione di lavoro è possibile:

scrivere il messaggio;

- associare al messaggio l'identificativo del destinatario o una lista di distribuzione;
- allegare, se necessario, un qualsiasi documento prodotto con l'elaboratore testi o con il foglio elettronico;
- inviare il messaggio oppure inserirlo in una bacheca comune.

Il servizio è immediato: dopo qualche istante il sistema di distribuzione inoltra la posta e la rende disponibile al destinatario o alla lista dei destinatari.

Viceversa il destinatario, una volta ricevuto il messaggio, può archiviarlo, cancellarlo e, eventualmente, inoltrare una risposta al mittente;

Indipendentemente dalla PDL è molto importante, per la ricezione di una comunicazione e quindi per il funzionamento logico dell'intero sistema, la verifica giornaliera della presenza o assenza di messaggi nella casella postale. Se non si effettua tale verifica, infatti, può accadere che il mittente sia costretto a ripetere la comunicazione con supporti tradizionali.

1.12SICUREZZA INFORMATICA

I SISTEMI INFORMATIVI SONO SICURI
OBIETTIVI DELLA SICUREZZA INFORMATICA

• Proteggere i sistemi fisici della struttura informatica contro eventi naturali, accidentali, fortuiti o intenzionali • Assicurare l'integrità e la riservatezza dei dati e delle informazioni • Garantire un adeguato livello di servizio e la disponibilità delle risorse (dati, programmi, ecc.) in presenza di eventi perturbativi.

Negli ultimi anni, quindi, il problema della Sicurezza nei sistemi informativi ha assunto un'importanza sempre crescente con l'evoluzione e lo sviluppo di basi dati integrate, di sistemi con terminali interattivi a disposizione di molti utenti con esigenze diversificate, di complessi sistemi distribuiti e, recentemente, delle reti di elaboratori.

L'insieme delle attività finalizzate alla tutela delle persone e dei beni sopraindicati si raggruppa nell'unica "*Funzione Sicurezza*" che acquista, quindi, precisi compiti e responsabilità.

1.13ARCHITETTURA DELLA RETE

La vecchia architettura di rete di telecomunicazioni prevedeva la seguente articolazione:

- Primo Livello, per il collegamento dei poli dipartimentali ai nodi della RUPA, tramite PVC (Private Virtual Circuit) con protocollo Frame Relay implementati su circuiti CDN urbani. Presso gli ex Provveditorati agli Studi (oggi C.S.A.) sono utilizzati, quali apparati RAS, degli Access Server Cisco modello AS 5300 60/12 modem già dotati di interfaccia sia per collegamenti analogici tramite RTN che per collegamenti digitali tramite ISDN.
- Secondo Livello, per il collegamento delle scuole agli ex Provveditorati agli Studi (oggi C.S.A.) di competenza, tramite connessioni in linea commutata digitale ISDN che consentono una velocità di trasferimento di almeno 64 kbps. Il sistema è stato dotato dei necessari requisiti di sicurezza (CUG) in grado di impedire accessi non autorizzati. Per ogni scuola è previsto un collegamento di un'ora per 250 giorni all'anno nonché un livello di contemporaneità degli accessi pari ad almeno 1/3 del numero di scuole. Sulle PdL in dotazione alle scuole sono installate schede ISDN di tipo Eicon Diva Pro 2.0 con bus PCI.

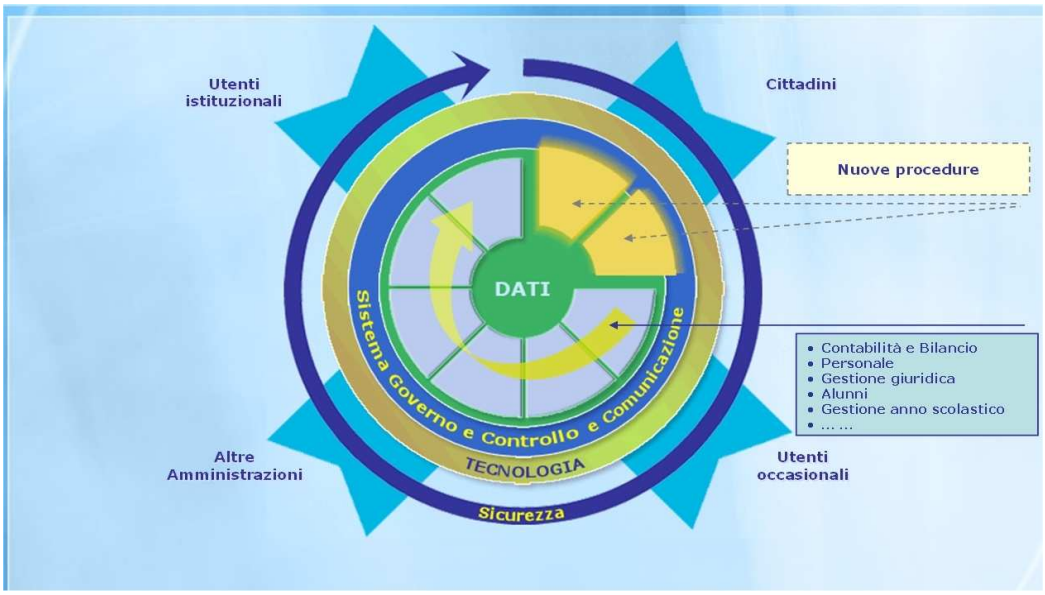
Attualmente (marzo 2009) là dove possibile, sono state sostituite tutte le linee ISDN con linee ADSL e sostituiti i relativi apparati di comunicazione.

1.14FLUSSO ATTUALE DELLE INFORMAZIONI

Il collegamento delle scuole consente il passaggio, per tutte le figure operanti nelle Direzioni Regionali, dalle attività di gestione del dato a quelle di miglioramento della qualità del servizio, controllo dell'integrazione ed elaborazione del dato.

Inoltre, la maggiore efficienza ed efficacia nell'organizzazione del servizio, consentirà ai livelli direttivi dell'Amministrazione Periferica di dedicarsi maggiormente allo svolgimento della loro funzione di supporto alle attività di governo e controllo della politica scolastica ("attività gestionali").

Complessivamente, anche i livelli direttivi dell'Amministrazione centrale avranno sempre più spazio per svolgere la loro funzione di pianificazione e controllo strategico (attività di "governo del processo").



1.15L'ORGANIZZAZIONE DEL SERVIZIO

Organizzazione del servizio in base alle disposizioni della legge 241/90: dare visibilità all'esterno della propria struttura organizzativa.

Piena visibilità della struttura organizzativa dell'Amministrazione, economicità ed efficacia come espresso dalla legge 241/90 sulla trasparenza.

Automazione efficiente.

Disponibilità delle informazioni (immediata reperibilità dei dati e continuità del servizio)

Indipendenza (autonomia di ricerca e garanzia alla riservatezza di chi interroga)

Identificazione univoca da parte dell'utente dell'autorità di riferimento.

Per rispondere alle disposizioni di legge in tema di trasparenza e orientamento al servizio (legge 241/90 e successive modificazioni) è necessario che l'Amministrazione fornisca all'utente la piena visibilità della sua struttura organizzativa. Per soddisfare questa esigenza non è sufficiente, però, il solo contributo degli impiegati dell'Ufficio per le Relazioni con il Pubblico.

Infatti, sia per ragioni legate alla disponibilità delle informazioni (immediata reperibilità dei dati e continuità del servizio) sia per motivi di indipendenza (autonomia di ricerca e garanzia alla riservatezza di chi interroga) si reputa necessario non vincolare il cittadino alla sola informazione assistita da addetti ma veicolarla anche attraverso l'utilizzo di strumenti informativi alternativi

I dati relativi all'organizzazione dovranno essere tali da favorire il cittadino nell'esercitare i propri diritti in merito alle procedure amministrative che lo

riguardano (sia a istanza di parte, sia d'ufficio) identificando univocamente l'autorità di riferimento. Per tale ragione i dati significativi devono comprendere:

- la denominazione delle unità organizzative (direzione, divisioni, uffici, etc.);
- le competenze degli uffici;
- i nominativi dei responsabili delle unità organizzative;
- la localizzazione degli uffici (strada e numero civico);
- la raggiungibilità telematica degli uffici (numeri telefonici e dei fax delle segreterie degli uffici);
- la raggiungibilità degli uffici (mezzi di trasporto dalla sede istituzionale e da punti di riferimento territoriali).

L'informativa sull'organizzazione deve riguardare sia la componente centrale che quella periferica (Sovrintendenze e Provveditorati). Al fine, però, di non incorrere in sovrapposizioni ed in conflitti di competenze, tale informativa a livello centrale dovrà essere limitata allo smistamento dell'utenza verso l'amministrazione periferica competente, fornendo esclusivamente i recapiti (indirizzo, telefono, fax) di interesse.

L'insieme delle informazioni relative all'organizzazione del Ministero rappresenta, in definitiva, anche una sintesi di cultura civica, di immediata e facile consultazione, a disposizione di scolaresche e di quanti fossero interessati.

Per quanto riguarda l'informazione sull'organizzazione del Ministero, i chioschi si delineano come strumenti importanti per guidare l'utente alla risoluzione di procedimenti di proprio interesse, in ragione di immediatezza, flessibilità, autonomia e oggettività.

L'informazione così veicolata completa quella relativa allo svolgimento delle procedure di competenza dell'amministrazione. Dà infatti la possibilità di raggiungere direttamente l'unità organizzativa di riferimento.

1.16LE FUNZIONI INTEGRATE DEL SISTEMA

L'obiettivo delle funzioni integrate del nuovo sistema è quello di fornire all'utenza finale un servizio sempre più efficiente ed efficace e di ottenere riflessi positivi immediati sull'attività lavorativa degli uffici stessi anche in base ai cambiamenti in atto (maggiore autonomia, decentramento, ecc.)

le funzioni che consentono la gestione amministrativa, contabile e giuridica del personale della scuola sono state inizialmente rilasciate per il personale docente della scuola primaria e successivamente per il restante personale della scuola (docente, direttivo e amministrativo, tecnico, ausiliario).

In particolare:

- integrazione informativa del rapporto Personale Scolastico / Amministrazione che ha costituito il fascicolo personale elettronico;
- gestione delle posizioni di stato che alimentano il fascicolo personale con gli atti di natura giuridica che caratterizzano il rapporto di lavoro con l'Amministrazione e gestione di tali informazioni ai fini della gestione del posto in organico di diritto e di fatto, della carriera e degli effetti contabili;

- attività propedeutiche all'avvio dell'anno scolastico, con l'obiettivo di garantire gli strumenti e l'organizzazione più adeguata per un tempestivo inizio delle attività scolastiche;
- gestione della dotazione organica e dei movimenti del personale per tutti gli ordini scuola e per tutte le tipologie di personale;
- contabilità speciale per una gestione degli adempimenti contabili correlati al pagamento degli stipendi dei maestri elementari in un contesto di integrazione dei procedimenti amministrativi;
- integrazione delle informazioni presenti nel fascicolo personale elettronico mediante i dati relativi alla formazione professionale e ai servizi comunque prestati; tale tipologia di dati verrà integrata con quanto già presente nel S.I.D., mediante uno scambio di informazioni con le banche dati dell'INPS;
- gestione della ricostruzione carriera e del trattamento di quiescenza mediante le informazioni di carriera presenti nel fascicolo personale elettronico e integrazione con le informazioni presenti nelle banche dati dell'INPS per consentire una liquidazione della pensione definitiva contestuale alla cessazione del rapporto di lavoro;
- applicazioni che rendono operativa la configurazione telematica che prevede il colloquio delle Segreteria Scolastiche e degli Uffici del Provveditorato con il Sistema Centrale e l'utilizzo delle funzioni e servizi offerti dal sistema stesso (informazioni di interesse del personale in servizio, dati relativi alla costituzione delle commissioni giudicatrici degli esami di maturità, risultati delle procedure di mobilità, stato di avanzamento delle pratiche di gestione giuridica);
- gestione delle tipiche attività locali delle segreterie scolastiche (di ogni ordine e grado); acquisizione delle informazioni che si originano nelle stesse scuole servizi prestati, assenze, situazioni familiari, dati professionalità, posti disponibili inorganico di diritto e di fatto, domande presentate dal personale) e trasmissione delle stesse al sistema;
- nell'ottica del miglioramento del servizio offerto dall'Amministrazione all'utente e al cittadino: sono state allestite, presso gli uffici centrali e periferici dei provveditorati, una serie di funzioni finalizzate allo snellimento delle procedure burocratiche manuali; aperti Uffici per le Relazioni al Pubblico che consentono la diffusione di informazioni di carattere generale (costituzione delle commissioni per gli esami di maturità e materie d'esame, dislocazione delle scuole, informazioni su docenti, A.T.A. e direttivi, movimenti, pratiche di pensione, riscatto e ricongiunzione);
- costituzione della banca dati delle strutture edilizie ad uso scolastico e futuro collegamento con il sistema utilizzato dagli uffici della Direzione Generale del Catasto;
- applicazioni di supporto alle attività decisionali delle Direzioni Generali (S.S.D.) mediante la costituzione di una banca dati storico-statistica e

generazione di modelli previsionali e decisionali. per rilevare situazioni critiche del sistema scuola in relazione al contesto socio-economico.

1.17SETTORI DI APPLICAZIONE

Per poter garantire l'ìntegrazione con gli altri sistemi informatici e le banche dati, il S.I.D. (Sistema informativo decentrato) è stato suddiviso nei seguenti settori d'intervento:

- Sistema di supporto alle decisioni (S.S.D.)
- Gestione Amministrativa
- Gestione Giuridica
- Organizzazione ed automazione dell'Ufficio
- Integrazione con altri sistemi.

Gestione Contabile
Automazione d'ufficio
Automazione dell'unità scolastica

IL S.I.D. È STATO MESSO A PUNTO, SIA MEDIANTE UN ADEGUAMENTO TECNICO, FUNZIONALE ED ORGANIZZATIVO DEL SISTEMA INFORMATIVO ESISTENTE CON AMPLIAMENTO E POTENZIAMENTO DELLE FUNZIONALITÀ, SIA CON LA REALIZZAZIONE DI NUOVE FUNZIONALITÀ.

1.18SISTEMA DI SUPPORTO ALLE DECISIONI

IN CHE MODO IL SISTEMA INFORMATIVO È IN GRADO DI SUPPORTARE IL LAVORO?

Migliora la visibilità dei parametri di funzionamento dell'apparato scolastico e mette in grado di operare tempestivamente le opportune scelte sulla base dei dati che scaturiscono dal vissuto del mondo scolastico.

Il settore si articola in diverse aree di intervento:
Modelli previsionali
Sottosistema storico-statistico
Il Sistema di Supporto alle Decisioni

Scopo del settore

Migliorare la visibilità dei parametri di funzionamento dell'apparato scolastico e operare tempestivamente le opportune scelte sulla base dei dati che scaturiscono dal vissuto del mondo scolastico.

Il settore si articola in diverse aree di intervento:

Modelli previsionali

Fornire strumenti per il controllo della realtà scolastica attraverso la previsione della dinamica evolutiva delle entità: alunni, classi, cattedre (posti), scuole, personale, costi, al fine di ipotizzare ed analizzare gli esiti di possibili scelte ed interventi.

Sottosistema storico-statistico

Soddisfare tempestivamente le esigenze conoscitive ed agevolare le attività di governo del fenomeno scolastico per i diversi livelli decisionali dell'Amministrazione centrale e Periferica:

- offrendo un quadro ordinato e sistematico della situazione di fatto, della dinamica degli eventi e dei legami esistenti fra le molteplici variabili del sistema;
- consentendo, in modo semplice ed in tempi brevi, di accedere alle informazioni necessarie al processo conoscitivo-decisionale;
- "navigando" sulla normativa primaria e secondaria e sui dati provenienti dalle procedure gestionali mediante "Sistemi Esperti" finalizzati alla risoluzione di problematiche amministrative, giuridiche e contabili.

1.19GESTIONE GIURIDICA

IN CHE MODO IL SISTEMA CONTRIBUISCE ALLA GESTIONE GIURIDICA?

1. disporre i dati del dipendente
2. sin dall'inizio della sua carriera
3. nella forma più elementare possibile.

PER UN CORRETTO E SNELLO SVOLGIMENTO DEGLI ADEMPIMENTI DI NATURA GIURIDICA

Integrazione informativa del rapporto personale scolastico Amministrazione

Gestione delle posizioni di stato del personale scolastico

Ricostruzione della carriera, riscatti e ricongiunzione dei periodi contributivi, trattamento di fine rapporto.

Scopo del settore

Disporre i dati del dipendente, sin dall'inizio della sua carriera, nella forma più elementare possibile onde consentire uno sviluppo di procedure modulari e con caratteristiche di elevata adattabilità sia alle modifiche della normativa

primaria e secondaria, sia alla interpretazione degli organi di controllo; tutto questo per un corretto e snello svolgimento degli adempimenti di natura giuridica.

Il settore si articola nelle seguenti aree di intervento: **Integrazione informativa del rapporto personale scolastico/Amministrazione.**

Creare una osmosi informativa tra le diverse aree d'intervento eliminando le ridondanze dei dati e garantendo più elevati livelli di efficienza funzionale attraverso:

- l'impianto e la tenuta del fascicolo personale;
- lo scambio informativo tra i settori amministrativo, giuridico e contabile;
- la gestione della professionalità e la formazione di commissioni d'esame;
- la distribuzione delle applicazioni ai diversi livelli;
- la storicizzazione delle informazioni.

Gestione delle posizioni di stato del personale scolastico

Gestire il rapporto di lavoro tra personale scolastico ed amministrazione in merito al complesso degli eventi che caratterizzano il servizio del dipendente, quali:

- conferimento delle supplenze;
- perfezionamento del rapporto giuridico di ruolo;
- variazioni di stato;
- interruzione definitiva del rapporto di impiego.

Tutto questo anche attraverso la costituzione di una base informativa dei procedimenti di stato giuridico e dei relativi iter.

Ricostruzione della carriera, riscatti e ricongiunzione dei periodi contributivi, trattamento di fine rapporto.

Gestire in modo integrato gli adempimenti per il riconoscimento dei servizi, di ruolo e non di ruolo prestati dal dipendente ai fini della carriera, della quiescenza e della previdenza con tempestiva produzione dei provvedimenti di:

- riconoscimenti dei servizi e benefici;
- inquadramento;
- riscatto;
- ricongiunzione;
- pensione definitiva.

Tutto questo anche al fine di effettuare un parziale recupero delle situazioni pregresse ed eliminare il fenomeno di "pensione provvisoria".

1.20ORGANIZZAZIONE E AUTOMAZIONE D'UFFICIO

IN CHE MODO IL SISTEMA PUO' SUPPORTARE IL LAVORO D'UFFICIO?

Obiettivi:

1. automatizzare le attività di carattere generale degli Uffici centrali e Periferici del Ministero

2. migliorare la qualità e la produttività del lavoro negli Uffici centrali e periferici del M.P.I.
3. gestire automaticamente l'iter delle pratiche
4. introdurre nuovi modelli organizzativi
5. integrare i contenuti informativi gestiti nell'ambito delle attività d'ufficio con le aree giuridiche amministrative e contabili.

Scopo del settore

- Automatizzare le attività di carattere generale degli Uffici centrali e Periferici del Ministero, ovvero riconfigurare l'insieme di tali attività (produzione documenti, gestione delle pratiche, archiviazione atti, organizzazione riunioni, ecc.) demandando all'automazione quelle più ripetitive, garantendo il più possibile l'omogeneità dei comportamenti e consentendo di rilevare dati sintetici utili ai fini di una migliore organizzazione e direzione delle attività stesse.
- Automatizzare le attività relative alla gestione degli organi collegiali e quelle connesse con la gestione amministrativa, contabile del personale amministrativo del Ministero.
- Migliorare la qualità e la produttività del lavoro negli uffici Centrali e Periferici del M.P.I. mediante l'impiego di tecnologie di automazione d'ufficio.
- Gestire automaticamente l'iter delle pratiche.
- Introdurre nuovi modelli organizzativi.
- Integrare i contenuti informativi gestiti nell'ambito delle attività d'ufficio con le aree giuridiche amministrative e contabili.

2.La rete unitaria della P.A.

2.1 IL CAMBIAMENTO DELLA P.A.

NELLA PUBBLICA AMMINISTRAZIONE

PROCESSI EVOLUTIVI IN ATTO

Aumento qualità ed efficienza

Nascono nuovi ruoli che comportano maggiori responsabilità per tutte le figure coinvolte

Tra i fattori critici del cambiamento occupa sicuramente un posto di rilievo l'introduzione delle nuove tecnologie che favoriscono la comunicazione ed il lavoro collaborativi. Tale innovazione da una parte

impone la riorganizzazione dei ruoli e dei processi e dall'altra parte si pone come volano del cambiamento.

Alcuni tra i principali fattori che spingono verso il cambiamento sono oggi:

1. I cittadini chiedono servizi migliori ed un migliore rapporto con gli uffici cui si rivolgono.
2. I dirigenti ed i funzionari pubblici sono fortemente orientati a snellire la burocrazia, cercando di risolvere i problemi ad essa connessi.
3. Il mondo produttivo esige procedure più efficienti ed efficaci, per garantire qualità e costi concorrenziali.
4. Le nuove tecnologie consentono e promuovono comportamenti organizzativi profondamente diversi, annullano vincoli di spazio e di tempo e creano maggiore trasparenza
5. Il mondo politico, con l'emanazione di nuove leggi, cerca il consenso dei cittadini e dei media, anche attraverso la modernizzazione degli uffici pubblici. Le nuove leggi, inoltre, sono i paletti di riferimento per il cambiamento.
6. L'UE e la comunità internazionale operano frequenti confronti sul funzionamento della macchina burocratica, sulle cause di inflazione, sugli sprechi, sulla modernità dei Paesi e sulla capacità di rispondere adeguatamente alle richieste di ogni Paese.

2.2 NASCE L'AIPA

La complessità e la grande articolazione dei servizi della Pubblica Amministrazione richiede oggi interventi e attività sempre più coordinate e integrate.

È necessario introdurre le tecnologie informatiche finalizzate all'aumento di efficacia ed efficienza dei servizi stessi.

L'Autorità per l'informatica nella Pubblica Amministrazione, nota anche come AIPA, è una autorità indipendente istituita dal decreto legislativo n. 39 del 12 febbraio 1993 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche" (come modificato dall'art.42 della legge 31 dicembre 1996, n.675) cioè un'amministrazione pubblica che prende le proprie decisioni in base alla legge, senza rapportarsi direttamente al governo o del Parlamento. L'Autorità è un organo formato da cinque persone, che prendono decisioni Collegialmente o a maggioranza I suoi membri sono nominati dal presidente del Consiglio, su proposta del presidente dell'Autorità, previa deliberazione del Consiglio dei Ministri.

2.3 COMPITI DELL'AIPA

L'autorità per l'informatica nella pubblica amministrazione favorisce l'integrazione e l'interconnessione dei sistemi informativi delle pubbliche amministrazioni, anche attraverso l'emanazione di norme tecniche e criteri per la progettazione e la gestione dei sistemi informativi automatizzati pubblici.

Favorendo così

IL MIGLIORAMENTO DEI SERVIZI PUBBLICI, IL CONTENIMENTO DEI COSTI DI GESTIONE E LA TRASPARENZA DELL'AZIONE AMMINISTRATIVA.

Queste fondamentali funzioni sono state arricchite e potenziate da numerose norme successivamente intervenute per definire nuovi compiti, consultivi, regolamentari, di coordinamento e d'impulso, nell'ambito del processo di ammodernamento delle pubbliche amministrazioni, connesso con l'introduzione, sempre più consistente, delle tecnologie dell'informazione come ad esempio il monitoraggio dei progetti informatici.

2.4 IL PROGETTO PORTANTE

Il progetto portante che accompagnò la nascita dell'AIPA

fu quello di creare una rete unitaria della Pubblica Amministrazione (RUPA)

che consentisse l'interoperabilità e l'interconnessione tra le varie amministrazioni, per superare la mancanza di integrazione che caratterizzava i sistemi informativi di

È evidente che la nascita della Rete comporti un profondo cambiamento culturale, sia all'interno delle Amministrazioni che all'esterno nel contesto sociale. In particolare ciò comporta:

1. La **cultura**, ossia la conoscenza da parte dei dirigenti pubblici delle potenzialità delle risorse informative e delle telecomunicazioni, in modo tale da poter riorganizzare il lavoro delle loro strutture.
2. Il **knowledge management**, ossia la integrazione delle dinamiche organizzative, della reingegnerizzazione dei processi e delle tecnologie; tutti questi elementi, infatti, contribuiscono in modo cooperativo ad ottimizzare ed a migliorare il recupero e la circolazione dei dati, delle informazioni e delle conoscenze rilevanti per

l'organizzazione e farle pervenire agli individui ed ai gruppi impegnati in compiti specifici.

3. La **conoscenza** specialistica, ossia lo sviluppo delle competenze tecniche di coloro che devono garantire l'efficienza del sistema di rete e l'integrazione delle soluzioni informatiche.
4. La **utilizzazione**, ossia lo sviluppo della capacità, da parte degli utilizzatori, di accedere alle informazioni che servono attraverso le tecnologie migliorandone l'approccio e generando la necessaria confidenza con gli strumenti.

Inoltre:

tale Rete, mettendo a disposizione le informazioni residenti su tutti i data base, consentirà inoltre di fornire un servizio rapido e completo al cittadino anche *on line* direttamente da casa. Ad esempio la realizzazione di un'anagrafe virtuale, attraverso il collegamento di tutto il sistema delle anagrafi esistenti nel nostro Paese.

2.5 LA RETE UNITARIA

PERCHÈ NASCE LA RETE UNITARIA?

Coordinamento e accesso reciproco ai dati di tutta l'amministrazione

La rete unitaria della pubblica amministrazione è il primo e più importante progetto intersettoriale dell'Autorità per l'informatica.

Qualsiasi utente operante su di un sistema ad essa connesso possa accedere, ai dati ed altre procedure residenti su qualsiasi altro sistema connesso.

In modo indipendente alle reti attraversate e dalle tecnologie in esse impegnate.

PER FAR SI' CHE

Purché debitamente autorizzato ed in condizioni di sicurezza!

La Rete unitaria è dunque una tecnologia abilitante all'interoperabilità ed alla cooperazione tra sistemi informativi e costituisce un fattore decisivo per l'innovazione della pubblica amministrazione.

RAPPRESENTA DUNQUE UNO STRUMENTO PER GARANTIRE UNA POSSIBILITA' DI UTILIZZO COORDINATO E RECIPROCO DI TUTTI I DATI DELLA PUBBLICA AMMINISTRAZIONE E IL SUO UTILIZZO CONSENTE DI OTTENERE

EFFETTI SIGNIFICATIVI: SULL'EFFICIENZA DELLA PUBBLICA AMMINISTRAZIONE; SUI COSTI ORGANIZZATIVI DEI SERVIZI SULLA QUALITÀ DEI SERVIZI AI CITTADINI ED ALLE IMPRESE.

2.6 LO STUDIO DI FATTIBILITA'

Il progetto intersettoriale Rete unitaria della pubblica amministrazione, approvato a fine '95 da parte del Consiglio dei Ministri di una Direttiva che nasce con uno studio di fattibilità da parte dell'AIPA riguarda gli aspetti relativi all'interconnessione telematica e all'interoperabilità tra le reti che costituiranno la Rete unitaria.

Lo studio di fattibilità si è concluso il 31 gennaio 1996 con la redazione dei seguenti documenti: il documento "Studio di fattibilità della rete unitaria", gli Allegati Tecnici allo Studio di fattibilità, le considerazioni finali nelle quali sono esposti i vantaggi della Rete. Tali vantaggi possono essere trovati in approfondimento.

La realizzazione di una Rete unitaria della Pubblica amministrazione costituisce momento essenziale del processo di ammodernamento dell'Amministrazione pubblica da tempo avviato in coerenza con gli obiettivi posti dal decreto legislativo 12 febbraio 1993, n. 39.

La Rete unitaria consentirà al sistema informativo di ciascuna amministrazione l'accesso ai dati ed alle procedure residenti nei sistemi informativi delle altre, nel rispetto della normativa in materia dei limiti di accesso, di segreto e di tutela della riservatezza. La Rete offrirà un sistema informativo integrato che permetterà alle singole amministrazioni, da un lato, di "colloquiare" tra di loro per lo scambio di ogni documento e informazioni utili e, dall'altro, di proporsi verso la collettività come centro unitario erogatore di dati e prestazioni amministrative.

BENEFICI OTTENIBILI DALLA RETE UNITARIA E COSTI CORRELATI

In questo capitolo conclusivo dello Studio vengono discussi i benefici ottenibili dalla Rete unitaria della Pubblica Amministrazione, dapprima in forma generale e successivamente tramite un esame comparato con i costi di realizzazione.

La Rete unitaria come fattore di successo

Il progetto della Rete unitaria si presenta come il progetto di riferimento per tutti gli interventi che saranno attivati nei prossimi anni per la riorganizzazione della Pubblica Amministrazione italiana. La Rete, la cui architettura complessiva esalta i meccanismi di cooperazione interamministrativa, metterà a disposizione degli operatori della pubblica amministrazione, dei cittadini, delle organizzazioni produttive e dei servizi un grande potenziale di strumenti di interoperabilità e di cooperazione. Essa, infatti, per il modo in cui è concepita, rappresenta una occasione molto significativa per sostenere processi di riforma capaci di combinare recuperi di efficienza con incrementi di qualità delle prestazioni erogate. È noto, e lo si è spesso ribadito nelle linee strategiche emanate da questa Autorità, che tra i fattori che ostacolano sia i primi che i secondi ve ne

sono non pochi che dipendono dal modo in cui sono organizzati i sistemi informativi della Pubblica Amministrazione: la separatezza tra le varie Amministrazioni, l'eccessiva centralizzazione di ciascuna pubblica amministrazione e del suo sistema informativo, la scarsa capacità di innovazione della Pubblica Amministrazione.

Tali aspetti richiedono che si instauri una positiva influenza tra fattori in apparenza contraddittori:

1. la distribuzione di responsabilità e quindi di autonomia in ciascuna Amministrazione;
2. la integrazione delle varie Amministrazioni nei macro-processi attraverso cui la pubblica amministrazione eroga le sue prestazioni ed assolve ai suoi compiti;
3. la capacità di innovazione delle singole Amministrazioni relativamente ai loro compiti, ai processi di cui sono responsabili e quindi alla loro organizzazione, ma anche della pubblica amministrazione nel suo complesso rispetto alla sua articolazione in Amministrazioni diverse.

La Rete unitaria della Pubblica Amministrazione cambia radicalmente lo scenario descritto precedentemente. Essa infatti è una infrastruttura di comunicazione e di accesso alle informazioni che: offre direttamente servizi di interoperabilità alle singole Amministrazioni, a sostegno dei loro processi di decentramento e distribuzione delle responsabilità, e alla Pubblica Amministrazione nel suo complesso, a sostegno dell'efficacia dei processi inter-amministrativi che le consentono di avere comportamenti coerenti e coordinati.

- crea inoltre le condizioni per sviluppare applicazioni a sostegno della
- cooperazione tra le unità di una singola Amministrazione e tra le
- varie Amministrazioni.
- consente di creare applicazioni che non si limitano ad automatizzare le attività di raccolta, elaborazione, memorizzazione e ricerca delle informazioni, come fanno nella stragrande maggioranza gli attuali sistemi informativi della Pubblica Amministrazione italiana, ma sono di aiuto al coordinamento di queste attività nei procedimenti amministrativi, alla gestione delle eccezioni che in essi si verificano, alla integrazione tra macro-processi di Governo, di pianificazione e organizzazione e di gestione delle varie aree di servizio.

Come i capitoli precedenti hanno illustrato e documentato in modo approfondito, le opportunità che offre la Rete unitaria della pubblica amministrazione si possono cogliere se i sistemi informativi della Amministrazioni e le modalità con cui essi vengono sviluppati evolvono verso:

- una nuova architettura di sistema a diversi livelli che uniforma le reciproche interfacce dei singoli sistemi in uno strato da cui si accede ai servizi della Rete unitaria, e per loro tramite, agli altri sistemi informativi, e che struttura le applicazioni interamministrative da semplici schemi di integrazione e interfacciamento dei sistemi informativi delle Amministrazioni partecipanti a veri e propri sistemi integrati a seconda della loro natura, in accordo con le politiche di

migrazione dei sistemi informativi più avanzate e più diffuse nel mondo;

- una architettura delle applicazioni centrata sulla cooperazione tra i processi quando il loro obiettivo è migliorare i tempi di attraversamento e risposta della gestione operativa, una architettura applicativa centrata sui dati quando il loro obiettivo è migliorare la qualità dei processi di governo e di pianificazione e organizzazione, secondo le più aggiornate soluzioni standardizzate che il mercato propone, in accordo con l'emergente paradigma di sistemi informativi cooperativi;
- modalità di sviluppo e gestione dei sistemi informativi e delle applicazioni che li costituiscono che li pone sotto responsabilità chiare e trasparenti, con protocolli di coordinamento tra di esse razionali ed efficaci, cosicché la loro modularità rispetto al mutare delle esigenze dei loro utenti e rispetto al mutare delle caratteristiche della infrastruttura in cui sono immerse sia liberata da ogni vincolo burocratico e messa nelle condizioni di crescere progressivamente in accordo con la trasformazione delle funzioni sistemi informativi da fabbriche di software a servizi interni delle organizzazioni;
- un contesto di riferimento sul terreno del piano triennale dell'informatica pubblica, delle procedure di approvazione e controllo dei progetti di sviluppo di nuove applicazioni, delle priorità di investimento e di spesa, ed infine dei criteri di tariffazione dei servizi della Rete unitaria della pubblica amministrazione, capace di orientare i sistemi informativi della pubblica amministrazione verso un rapido e pieno sfruttamento dei servizi della Rete e, loro tramite, verso una cooperazione a connessione lasca che ne massimizzi la integrazione senza limitarne l'autonomia di sviluppo.

I progetti pilota, mentre mostrano quanto siano rilevanti le opportunità che la Rete offre alla pubblica amministrazione nel suo complesso e alle singole Amministrazioni sul terreno del miglioramento dell'efficacia dei loro processi verso i loro destinatari (clienti) interni e/o esterni, se i criteri sopra ricordati sono seguiti con rigore, ci dicono anche che la distanza che le Amministrazioni devono colmare per sfruttarle pienamente non è abissale, e che impegnandosi nella direzione indicata è possibile avere risultati significativi in tempi certi.

Ritornando alle tre parole chiave, **autonomia, integrazione e innovazione**, indicate in apertura di questo capitolo, è bene mettere in chiaro come i criteri illustrati in questo documento le armonizzano sciogliendo ogni possibile contraddizione tra loro:

- le architetture di sistema e applicative proposte combinano efficacemente la capacità di mantenere i sistemi informativi esistenti quali che siano le loro architetture con quella di ospitare applicazioni progettate secondo impostazioni innovative e originali, per cui esse orientano l'evoluzione dei sistemi informativi della pubblica amministrazione verso l'innovazione senza imporre loro difficilmente gestibili riscritture globali;

- la Rete unitaria della pubblica amministrazione, se interfacciata secondo la architettura di sistema proposta, rende possibile attivare autonomamente sia lo sviluppo di applicazioni interamministrative che quello di applicazioni interne ad una singola Amministrazione, per cui le singole Amministrazioni mantengono una autonoma responsabilità sui loro sistemi senza che l'esercizio di quest'ultima si opponga allo sviluppo di applicazioni che favoriscano e realizzino forme di integrazione e di cooperazione con le altre Amministrazioni;
- le raccomandazioni che abbiamo sottolineato sul processo di disegno e sviluppo delle nuove applicazioni e sulle modalità con cui vanno valutati i costi e i benefici che provocano, gli impatti sulle dimensioni normative, organizzative e professionali, danno ai termini autonomia e integrazione un significato non rituale, per cui lo sviluppo dei sistemi informativi delle singole Amministrazioni e della pubblica amministrazione nel suo complesso viene ricondotto alla responsabilità manageriale dei suoi dirigenti, liberandolo da ogni protezionismo di impianto tecnocratico. Andando nella direzione indicata in questo documento l'informatica pubblica assumerà pienamente un ruolo attivo nella promozione dell'auspicato cambiamento della pubblica amministrazione, evitando la ghettizzazione che oggi la isola.

Passando ad analizzare i benefici e i costi del progetto, si può anzitutto affermare che i principali benefici sono:

- benefici economici derivanti dalla razionalizzazione dei costi di comunicazione;
- benefici economici derivanti dalla riduzione delle attività oggi imputabili alla frammentazione dei processi di servizio e ai conseguenti costi di transazione;
- benefici economici per la Pubblica Amministrazione derivanti dalla integrazione dei processi, dalla diminuzione dei tempi di servizio, dalla migliore qualità dei prodotti intermedi e finali;
- benefici organizzativi dovuti al naturale riorientamento della struttura amministrativa verso il servizio, che le architetture di cooperazione impongono;
- benefici di relazione derivanti dall'aumento di visibilità sui procedimenti amministrativi con la piena attuazione della legislazione sulla trasparenza;
- benefici economici per le imprese ed i cittadini, che vengono sollevati
- dai costi di integrazione attualmente sopportati.

L'importanza quantitativa di tali benefici è intuibile sulla base dei seguenti elementi: circa l'85% dei processi di lavoro nella Pubblica Amministrazione centrale (calcolabili in circa ventimila) è attualmente non informatizzato. Di essi, circa l'80%, in virtù delle sue caratteristiche procedurali, può usufruire dei servizi di interoperabilità, mentre circa il 50% potrà essere migliorato mediante gli strumenti di cooperazione.

È ipotizzabile una significativa riduzione media dei tempi relativi ai processi interamministrativi e dei tempi spesi dai cittadini. È anche ipotizzabile un

significativo miglioramento della efficacia di molti processi di servizio. Per una valutazione precisa, relativa ai processi di singole amministrazioni o gruppi di amministrazioni, si preferisce responsabilmente rinviare la quantificazione dei benefici ad un successivo momento progettuale. Per il sistema paese nel suo complesso, oltre ai benefici derivanti dal minor costo e dalla maggiore efficienza dei servizi pubblici erogati a cittadini e imprese, è inoltre utile considerare l'effetto positivo che il progetto di rete unitaria avrà sull'intero settore industriale delle tecnologie dell'informazione e delle telecomunicazioni.

Lo sviluppo delle applicazioni di cooperazione amplierà infatti il mercato dei servizi applicativi con benefici effetti quantitativi su un settore fondamentale per il profilo industriale del paese, e, soprattutto, orienterà l'offerta delle imprese verso architetture di riferimento moderne ed adeguate ai prevedibili sviluppi tecnologici dell'informatica e delle telecomunicazioni, realizzando l'obiettivo di contribuire allo sviluppo industriale attraverso un miglioramento della qualità della domanda pubblica.

Gli aspetti economici

Una valutazione degli aspetti economici della realizzazione della Rete unitaria può essere fatta con riferimento alle tre aree relative ai servizi di trasporto, all'interoperabilità e alle applicazioni.

Per quanto attiene al trasporto, il ricorso ad un unico fornitore di servizi, previsto nell'ambito della Rete, con la conseguente razionalizzazione e semplificazione degli impianti consentirà di fruire di risparmi sui costi per le telecomunicazioni ipotizzabile, nell'ipotesi minima di mantenimento integrale delle attuali architetture, in circa 120 - 180 miliardi l'anno, a fronte di una spesa attuale di circa 600 miliardi.

Una completa migrazione verso soluzioni tecnologicamente più moderne porterà il risparmio a 250 - 350 miliardi l'anno.

Gli interventi nell'area dell'interoperabilità comportano la realizzazione di nuovi impianti e l'erogazione di nuovi servizi in quanto si riferiscono a funzionalità della Rete unitaria che gli attuali sistemi informativi non forniscono. L'onere finanziario per la realizzazione del Centro Tecnico di Assistenza e l'esercizio dei servizi di interoperabilità è stimabile in 50 miliardi l'anno.

Il completo raggiungimento dei benefici attesi dalla Rete unitaria potrà ottenersi soltanto attraverso la realizzazione dei servizi di cooperazione. A questo proposito, lo studio ha definito una architettura di cooperazione a tre livelli, e ha individuato un insieme prioritario di aree, per le quali sono stati indicati possibili interventi tecnici e organizzativi.

Gli obiettivi dello studio per la parte relativa ai servizi di cooperazione, non rientravano nel mandato così come delineato dalla Direttiva, e sono stati perciò circoscritti ad una prima ricognizione delle problematiche architetturali ed applicative.

Nell'ambito del prossimo triennio ogni amministrazione potrà procedere all'adeguamento delle applicazioni esistenti e alla individuazione di nuove applicazioni, partecipando al progetto secondo la seguente tempistica: 1997 - Ciascuna amministrazione definirà l'insieme dei servizi (dati e applicazioni) che

intende esportare verso le altre amministrazioni, precisando il livello di sicurezza richiesto, e l'insieme dei servizi che intende importare dalle altre amministrazioni.

La complessità delle questioni affrontate, e la relativa indeterminatezza degli aspetti progettuali, richiedono una responsabile prudenza nella valutazione delle risorse economiche e finanziarie necessarie alla attuazione del progetto di cooperazione applicativa. Alla data odierna, sulla base degli elementi di stima disponibili, le risorse necessarie possono orientativamente quantificarsi in circa 350 miliardi all'anno per tre anni, corrispondenti ad un incremento del 10% dell'attuale spesa informatica nella Pubblica Amministrazione, essendosi ipotizzato che le economie derivabili dal servizio di trasporto siano investite in acquisizioni di apparecchiature informatiche.

2.7 BREVE STORIA

QUALE È STATA LA STORIA DEL PROGETTO RUPA?

Alla nascita dell'AIPA fu subito evidente la necessità di procedere rapidamente ad un profondo rinnovamento dei sistemi informativi della P.A. tale necessità ha fatto nascere il progetto della Rete Unitaria.

Ripercorriamo rapidamente i passi che hanno portato alla sua nascita:

giugno 1994: viene emanato il rapporto Bangermann "L'Europa e la società dell'informazione".
1994/1995: vengono intraprese alcune attività, tra le quali, una rilevazione dello stato delle reti di telecomunicazione della pubblica amministrazione centrale e degli enti pubblici non economici, e la formulazione di un modello del traffico dei dati, in grado di produrre stime di carico della futura rete.
Maggio 1995: l'Autorità invia al Governo, un documento che delineava nei suoi elementi essenziali, le caratteristiche della Rete Unitaria.
Febbraio 1996: viene pubblicato lo studio di fattibilità della Rete.

Giugno 1994: il rapporto Bangemann ("L'Europa e la società dell'informazione"), nel portare l'attenzione del Consiglio Europeo sugli sviluppi che il mercato dell'ICT in Europa stava conoscendo, formulava raccomandazioni pienamente in linea con gli scopi della Rete unitaria:

- "L'interconnessione delle reti e l'interoperabilità dei servizi e delle applicazioni devono essere obiettivi primari per l'Unione".
- "Il Gruppo raccomanda un'azione urgente e coerente sia a livello europeo che dei Paesi membri per promuovere la disponibilità e un uso esteso a livello europeo di servizi di base standard, come la posta elettronica, il trasferimento di file e i servizi video".
- "Reti amministrative trans-europee: un governo migliore e meno costoso".

1994/1995: vengono intraprese alcune attività, tra le quali, una rilevazione dello stato delle reti di telecomunicazione della pubblica amministrazione

centrale e degli enti pubblici non economici, e la formulazione di un modello del traffico dei dati, in grado di produrre stime di carico della futura rete.

Maggio 1995: l'Autorità invia al Governo, un documento che delineava nei suoi elementi essenziali, le caratteristiche della Rete Unitaria. La direttiva del Presidente del Consiglio dei Ministri "Rete unitaria della pubblica amministrazione", approvata il 5 settembre 1995, fissò, sia le finalità del sistema che le fasi della sua realizzazione.

Febbraio 1996: viene pubblicato lo studio di fattibilità della Rete, predisposto con la collaborazione degli organi tecnici del Ministero delle poste e delle telecomunicazioni. Esso riguarda gli aspetti di interconnessione e di interoperabilità, delineando, inoltre, un'architettura complessiva della Rete, anche per quanto riguarda la cooperazione applicativa.

2.8 AIPA - CNIPA

AIPA - CNIPA

Ancora prima della "Legge Bassanini" con Decreto istitutivo D. L. vo 12 febbraio 1993, n. 39 (G.U. 20/2/1993, n.42) è stata istituita l'AIPA - **Autorità per l'informatica nella Pubblica Amministrazione** – che aveva all'origine il compito di "promuovere, coordinare, pianificare e controllare lo sviluppo di sistemi informativi automatizzati delle amministrazioni pubbliche, secondo criteri di standardizzazione, interconnessione ed integrazione dei sistemi stessi".

L'obiettivo da perseguire era quello del "miglioramento dei servizi, del contenimento dei costi e del miglioramento della trasparenza dell'azione amministrativa, del potenziamento dei supporti conoscitivi per le decisioni pubbliche".

Venivano anche indicati criteri e strumenti per favorire l'accesso ai siti web delle pubbliche amministrazioni e l'uso delle applicazioni informatiche da parte delle persone disabili.

In particolare, venivano specificati i criteri da rispettare nella progettazione e manutenzione dei sistemi informatici pubblici, per favorire l'accessibilità ai siti web. L'aspetto relativo alle "**Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici**" sarò poi ripreso nella legge ad hoc n° 4 del 9 gennaio 2004, comunemente chiamata "Legge Stanca".

L'**AIPA** è stata soppressa con la Legge 16 gennaio 2003, n. 3 e L'autorità è confluita nel CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione.)

Il **CNIPA** opera presso la Presidenza del Consiglio per l'attuazione delle politiche del Ministro per le riforme e le innovazioni nella PA. Unifica in sé due organismi preesistenti: l'Autorità per l'informatica nella pubblica amministrazione ed il Centro tecnico per la R.U.P.A. (Rete Unitaria Pubblica Amministrazione). Il CNIPA ha l'obiettivo primario di dare supporto alla pubblica amministrazione nell'utilizzo efficace dell'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa. In sintesi il CNIPA:

- contribuisce alla definizione della politica del Governo e del Ministro per le riforme e le innovazioni nella PA e fornisce consulenza per la valutazione di progetti di legge nel settore informatico;
- coordina il processo di pianificazione e i principali interventi di sviluppo; detta norme e criteri per la progettazione, realizzazione, gestione dei sistemi informatici delle amministrazioni, della loro qualità e dei relativi aspetti organizzativi; definisce criteri e regole tecniche di sicurezza, interoperabilità, prestazione;
- controlla che gli obiettivi e i risultati dei progetti di innovazione della pubblica amministrazione siano coerenti con la strategia del Governo; a tale scopo si affianca alle amministrazioni pubbliche nella fase di progettazione ed emette pareri di congruità tecnico-economica;
- cura l'attuazione di importanti progetti per l'innovazione tecnologica nella pubblica amministrazione, la diffusione dell'e-government e lo sviluppo delle grandi infrastrutture di rete del Paese per consentire agli uffici pubblici di comunicare tra loro e per portare i servizi della pubblica amministrazione ai cittadini e alle imprese;
- cura la formazione dei dipendenti pubblici nel settore informatico, utilizzando le nuove tecnologie per favorire l'apprendimento continuo.

Per **e-government** (anche e-gov o amministrazione digitale) si intende il processo di informatizzazione della pubblica amministrazione, il quale - unitamente ad azioni di cambiamento organizzativo - consente di trattare la documentazione e di gestire i procedimenti con sistemi digitali, grazie all'uso delle tecnologie dell'informazione e della comunicazione (ICT), allo scopo di ottimizzare il lavoro degli enti e di offrire agli utenti (cittadini ed imprese) sia servizi più rapidi, che nuovi servizi, attraverso - ad esempio - i siti web delle amministrazioni interessate. (Wikipedia).

Tra gli atti e le norme successive di maggiore importanza vanno certamente ricordate, perché coinvolgono profondamente il rapporto e l'operato della Pubblica Amministrazione:

- la riforma de titolo V della Costituzione;
- l'Istituzione del Sistema Pubblico di Connettività;
- l'emanazione del Codice dell'Amministrazione Digitale.

Il **Codice dell'Amministrazione Digitale** è stato emanato con Decreto legislativo del 7 marzo 2005, n. 82, pubblicato sulla Gazzetta ufficiale n. 111 del 16 maggio 2005, a seguito della delega al Governo contenuta all'articolo 10 della legge 29 luglio 2003, n. 229 (Legge di semplificazione 2001). Il Codice è entrato in vigore il 1 gennaio 2006. Esso ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione all'interno della pubblica amministrazione, nei rapporti tra amministrazione e privati e in alcuni limitati casi, disciplina anche l'uso del documento informatico nei documenti tra privati. Nel 2006, pochi mesi dopo l'entrata in vigore, il Codice è stato oggetto di una serie di correttivi, disposti con il decreto legislativo 4 aprile 2006, n. 159 la

cui emanazione era stata autorizzata dalla medesima legge-delega n. 229 del 2003. (Wikipedia).

2.9 SPC - Sistema Pubblico di Connettività

SPC - Sistema Pubblico di Connettività

Prima di entrare nella specificità della Scuola occorre spendere due parole sul Sistema Pubblico di Connettività che può essere definito come "l'insieme di strutture organizzative, infrastrutture tecnologiche e regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la circolarità del patrimonio informativo della pubblica amministrazione, necessarie per assicurare l'interoperabilità e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza e la riservatezza delle informazioni."

Il progetto è articolato in due fasi principali secondo due obiettivi:

- la definizione dell' SPC nel suo complesso, delle strutture organizzative per il suo governo, le infrastrutture tecnologiche e le regole tecniche per la fornitura dei servizi di connettività ed interoperabilità di base nel rispetto dei necessari requisiti di sicurezza;
- la definizione del modello e dei servizi di interoperabilità evoluta e cooperazione applicativa e lo sviluppo dell'architettura abilitante e delle relative regole di governo.

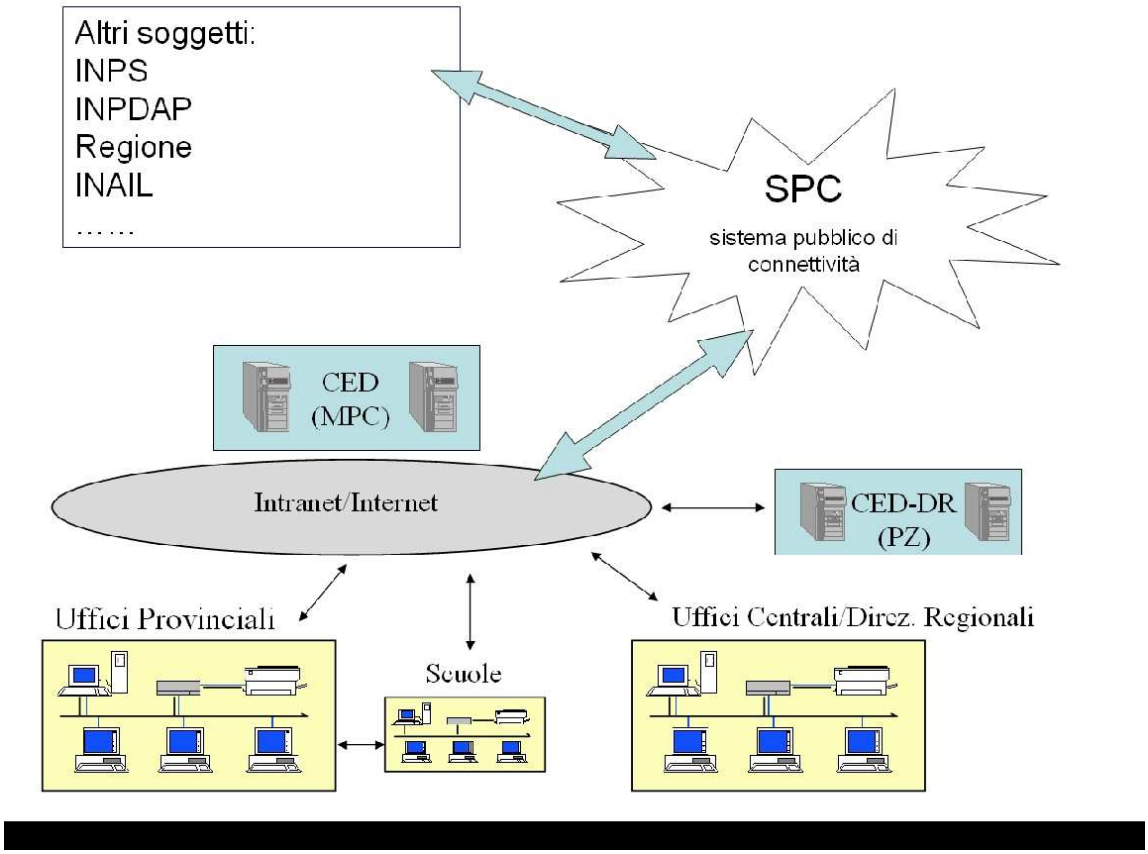
Principi di base:

1. Sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema.
2. *Economicità* nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa.
3. Sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.

Obiettivi:

- Fornire un insieme di servizi di connettività condivisi dalle Pubbliche Amministrazioni (PA) interconnesse, graduabili in modo da poter soddisfare le differenti esigenze.
- Garantire l'interazione della PA centrale e locale con tutti gli altri soggetti connessi a internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità per cittadini e imprese.
- Fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilità tra tutte le reti delle PA esistenti.
- Fornire servizi di connettività e cooperazione alle PA che ne facciano richiesta, per permettere l'interconnessione delle proprie sedi e realizzare così anche l'infrastruttura interna di comunicazione.
- Realizzare un modello di fornitura dei servizi multifornitore coerente con l'attuale situazione di mercato e le dimensioni del progetto stesso.

- Garantire lo sviluppo dei sistemi informatici nell'ambito del SPC salvaguardando la sicurezza dei dati, la riservatezza delle informazioni, nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni.



2.10 DI Scuola

Per quanto concerne il mondo della scuola ampie e profonde sono state le innovazione apportate rispetto alle modalità di lavoro che ai processi operativi nell'arco di questi ultimi anni; dalle applicazioni tipicamente basate su sistemi prima X25 o ISDN e poi su Web (SISSI - SIMPI ma ancora con interfaccia a caratteri) si è arrivati alle applicazioni con front-end grafico (GUI *graphical user interface*) su banda larga quale il nuovo sistema SIDI Scuola.

SIDI Scuola

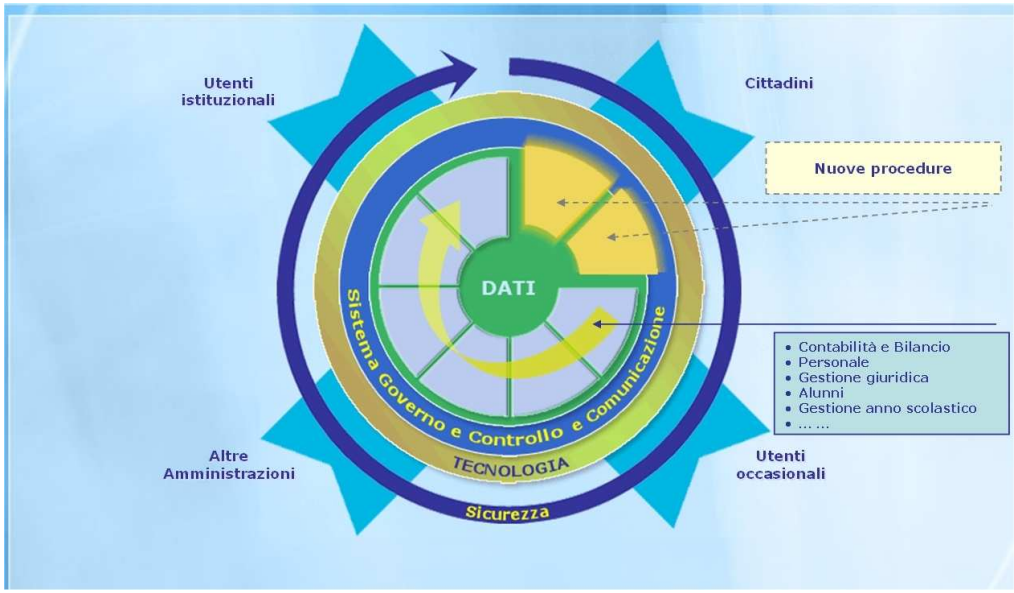
Il nuovo "Sistema Informativo dell'Istruzione (SIDI)" è stato concepito per valorizzare, attraverso un processo primario di modernizzazione tecnologica, l'intero patrimonio del MPI nei suoi molteplici aspetti:

- Finanziario, supportando in concreto la gestione e la pianificazione della spesa
- Relazionale, potenziando la capacità di ascolto e favorendo flussi comunicativi multidirezionali in una logica di rete
- Umano, migliorando e rendendo più efficace il modo in cui il personale del MPI lavora e collabora
- Informativo, consentendo la condivisione e la disponibilità delle informazioni
- Tecnologico, ammodernando le procedure informatiche di supporto e rinnovando l'intero "parco tecnologico"

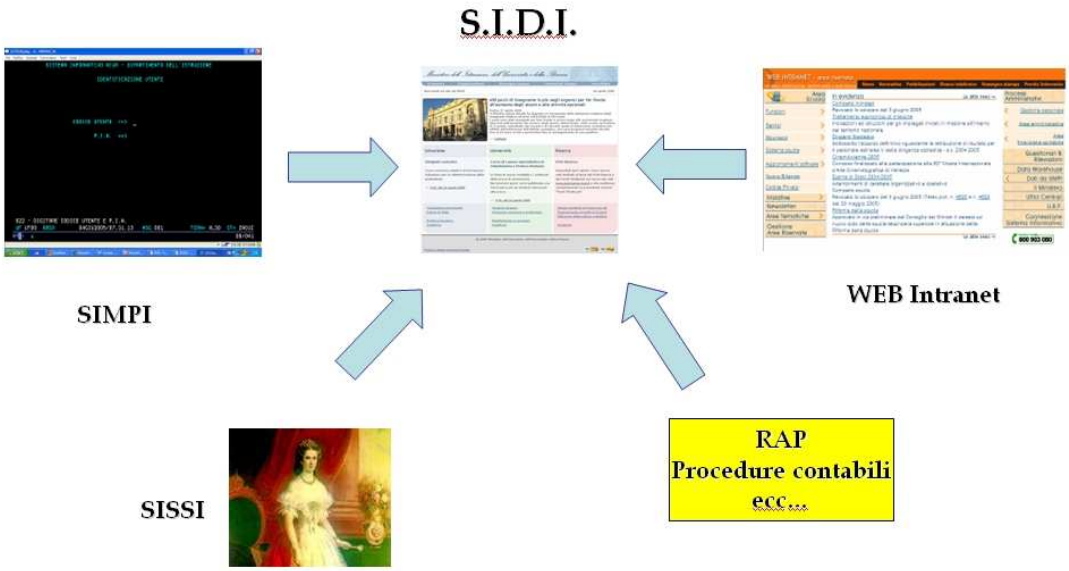
Il SIDI propone di garantire:

- Classificazione e controllo dei beni
- Protezione fisica e logica delle risorse
- Gestione dei supporti rimovibili
- Back-up delle informazioni
- Gestione degli scambi di sw e informazioni con enti esterni
- Utilizzo della crittografia e della firma digitale laddove appropriato
- Sicurezza dei sistemi di automazione di ufficio
- Gestione , monitoraggio, e controllo degli accessi degli utenti ai sistemi e alla rete
- Sviluppo e manutenzione dei sistemi
- Continuità dei servizi
- Verifica periodica di efficacia e di validità nel tempo delle contromisure adottate.

Il portale SIDI rappresenta lo strumento dal quale si accede al menù delle funzionalità del Sistema Informativo del Ministero della Pubblica Istruzione destinate agli Uffici Centrali e Periferici (USR, USP e istituzioni scolastiche).



La trasformazione del sistema



Accesso al sistema

Il Portale diventa il punto di accesso unico a tutti i servizi, sia per utenti istituzionali che esterni, e offre servizi differenziati in funzione delle autorizzazioni e del profilo dell'utente che accede.

Alcuni servizi …

A titolo esemplificativo si riportano alcuni dei servizi che il personale Amm.vo potrà essere chiamato a gestire:

- Anagrafe alunni
- Gestione del personale
- Gestione delle competenze
- Gestione giuridica (ricostruzione di carriera)
- Le assunzioni
- L'organico di diritto
- Bilancio nelle scuole
- Il Programma Annuale
- Variazioni del programma
- Fondo minute spese
- Ritenute e liquidazioni
- Conto Consuntivo
- Chiusura anno finanziario
- Funzioni di supporto
- Sicurezza e gestione delle utenze
- Gli esami di stato e di abilitazione alla libera professione
- Gestione schede e Gestione risultati di nomina

- Gestione schede
- Interrogazioni schede
- Stampa lettere di notifiche
- Gestione risultati di nomina
- Rilevazioni integrative
- …….. ……. …….

Dematerializzazione dei contratti – news – Circolare Interministeriale del 4 agosto 2008

http://www.pubblica.istruzione.it/demat/allegati/ci771.zip

Le scuole invieranno i contratti al Tesoro e alla Ragioneria esclusivamente via web; resteranno solo due copie cartacee, firmate dal dirigente e dal supplente. Si tratta di un progetto del MIUR e del MEF per velocizzare le fasi amministrative e ridurre la carta utilizzata.

Questo è solo il primo passo verso la completa sostituzione del contratto cartaceo con un il documento informatico sottoscritto con firma digitale che garantisca l'identificabilità dell'autore e l'integrità del documento

Fascicolo elettronico del personale

La gestione del fascicolo del personale come processo unico che permetta la disponibilità di uno "stato matricolare" conforme a requisiti di completezza, aggiornamento e fruibilità adeguati alla accresciute esigenze di granularità informativa.

Le Rilevazioni

Le Rilevazioni sono indagini che annualmente vedono tutte le scuole, statali e non statali, impegnate nella raccolta e comunicazione di dati di particolare interesse al sistema informativo centrale (alunni diversamente abili, alunni stranieri, esiti degli scrutini, esami di stato…) che non risultano disponibili.

Il patrimonio informativo del sistema, che è costituito da dati di carattere generale, viene così integrato e si arricchisce di notizie più specifiche: le Rilevazioni diventano, quindi, la base informativa essenziale per il monitoraggio del sistema scolastico educativo nazionale ed uno dei riferimenti su cui costruire le politiche scolastiche.

La procedura d'inserimento dei dati delle **Rilevazioni** è accessibile in modalità web sul portale dei servizi SIDI per tutte le scuole, statali e non statali, di tutti gli ordini. Il collegamento diretto al SIDI da parte di ogni singolo istituto, coadiuvato dai Referenti degli Uffici Scolastici Provinciali e Regionali, rende l'attività di rilevazione più razionale ed efficace.

Al fine di migliorare la coerenza dei dati richiesti alle scuole, le nuove Rilevazioni sono state progettate tenendo conto delle esigenze informative delle varie Direzioni Generali del Ministero così da evitare le ripetute richieste di dati e rendere minimo l'onere di risposta da parte delle scuole.

Struttura delle Rilevazioni

Le Rilevazioni si compongono delle seguenti tre aree:

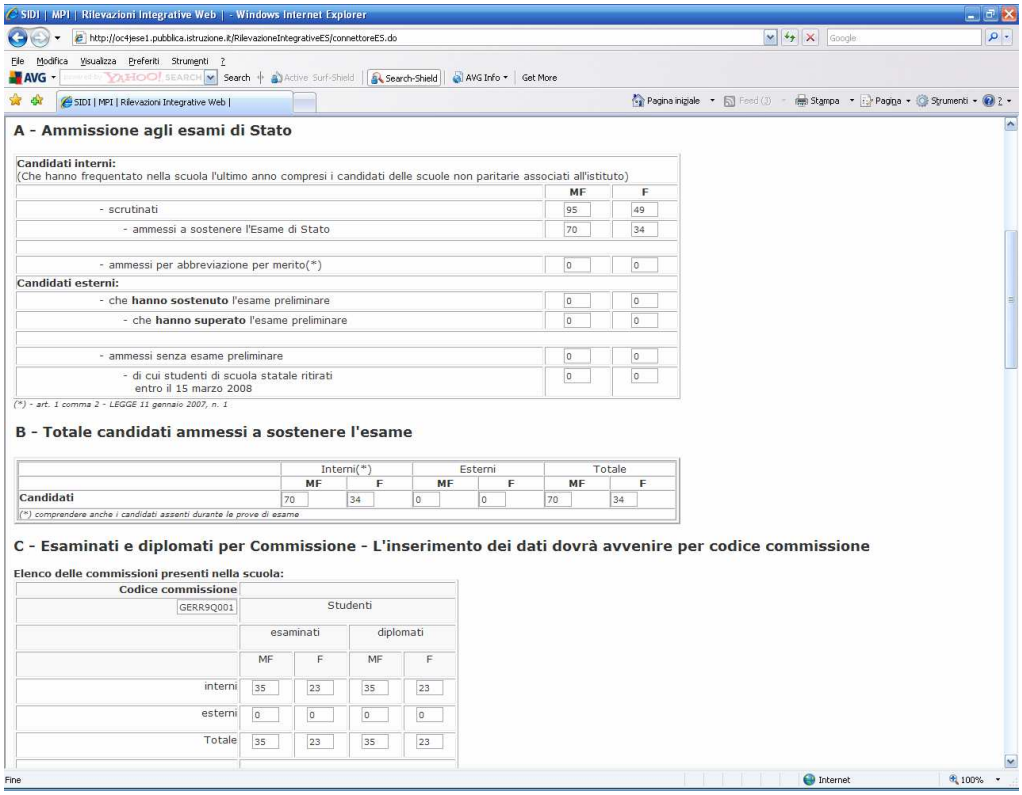
- Rilevazioni Integrative-Dati analitici delle scuole, rivolte a tutti gli ordini scuola
- Rilevazioni Esiti degli Scrutini Finali, rivolte alle scuole primarie, secondarie di I e di II grado
- Rilevazioni Esami di Stato, rivolte esclusivamente alle secondarie di II grado, statali e paritarie.

Come inserire i dati

Come per le Rilevazioni Integrative, la procedura per la trasmissione dei dati è possibile esclusivamente attraverso un'interfaccia WEB accedendo al portale dei servizi SIDI. L'inserimento dei dati avviene, sia per le scuole statali che per le scuole paritarie, autonomamente attraverso appositi moduli elettronici che consentono l'archiviazione automatica delle informazioni e controllano immediatamente la loro coerenza.

L'anagrafe degli alunni

Creazione di un'anagrafe nazionale alimentata raccogliendo i dati delle scuole e finalizzata alla costruzione del curriculum dello studente, che lo accompagni nel corso del suo iter scolastico.



2.11 SIDI Learn

SIDILearn è la piattaforma dedicata alla formazione del personale dell'amministrazione scolastica (a tutti i livelli). La formazione, erogata in modalità blended, anche con l'ausilio di strumenti di WBT (Web-Based Training) permette la fruizione di specifici corsi.

I corsi di formazione hanno l'obiettivo di fornire ai partecipanti una panoramica sulle funzionalità, sulle nuove modalità di interfaccia, sui cambiamenti di processo e di relazione con gli uffici centrali e territoriali dell' Amministrazione, sugli strumenti di gestione e di controllo che il nuovo SIDI mette a disposizione delle Istituzioni Scolastiche e dell'Amministrazione, nell'ambito dello snellimento delle procedure e della valorizzazione dell'intero patrimonio informativo del Ministero.

La piattaforma di formazione è suddivisa in aree tematiche: l'attività corsuale specifica, l'area FAQ (Frequently Asked Questions), l'area messaggistica, l'area novità.

Non manca su SidiLearn l'area FORUM per la libera discussione e per il confronto reciproco.

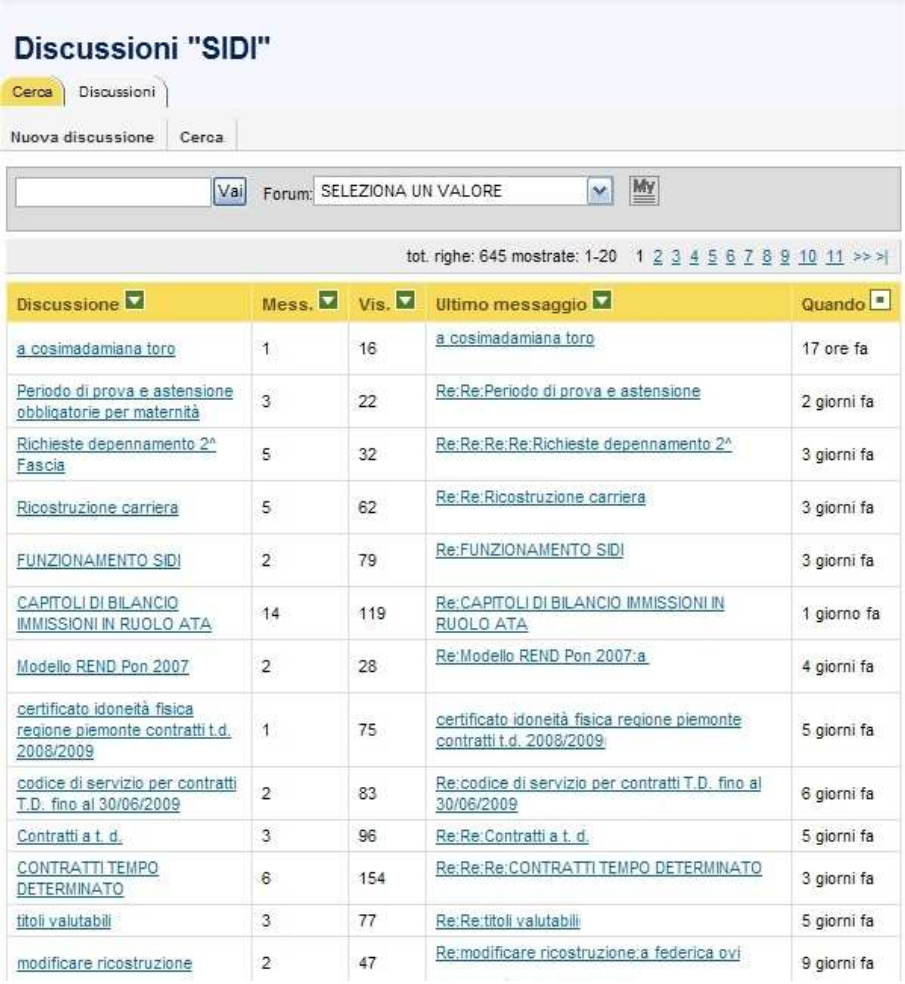
Sitografia

Decreto istitutivo AIPA Decreto Legislativo 12 febbraio 1993, n. 39 (G.U. 20/2/1993, n.42).

http://www.cnipa.gov.it/site/_contentfiles/00121000/121093_dlgs39_1993.PDF

Legge 15 marzo 1997, n. 59 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"

http://www.parlamento.it/leggi/97059l.htm



Discussione	Mess.	Vis.	Ultimo messaggio	Quando
a cosimadamiana toro	1	16	a cosimadamiana toro	17 ore fa
Periodo di prova e astensione obbligatorie per maternità	3	22	Re:Re:Periodo di prova e astensione	2 giorni fa
Richieste depennamento 2^ Fascia	5	32	Re:Re:Re:Re:Richieste depennamento 2^	3 giorni fa
Ricostruzione carriera	5	62	Re:Re:Ricostruzione carriera	3 giorni fa
FUNZIONAMENTO SIDI	2	79	Re:FUNZIONAMENTO SIDI	3 giorni fa
CAPITOLI DI BILANCIO IMMISSIONI IN RUOLO ATA	14	119	Re:CAPITOLI DI BILANCIO IMMISSIONI IN RUOLO ATA	1 giorno fa
Modello REND Pon 2007	2	28	Re:Modello REND Pon 2007:a	4 giorni fa
certificato idoneità fisica regione piemonte contratti t.d. 2008/2009	1	75	certificato idoneità fisica regione piemonte contratti t.d. 2008/2009	5 giorni fa
codice di servizio per contratti T.D. fino al 30/06/2009	2	83	Re:codice di servizio per contratti T.D. fino al 30/06/2009	6 giorni fa
Contratti a t. d.	3	96	Re:Re:Contratti a t. d.	5 giorni fa
CONTRATTI TEMPO DETERMINATO	6	154	Re:Re:Re:CONTRATTI TEMPO DETERMINATO	3 giorni fa
titoli valutabili	3	77	Re:Re:titoli valutabili	5 giorni fa
modificare ricostruzione	2	47	Re:modificare ricostruzione:a federica ovi	9 giorni fa

- Riforma titolo V della Costituzione - Legge costituzionale 18 ottobre 2001, n. 3, «Modifiche al titolo V della parte seconda della Costituzione» in GU n. 248 del 24 ottobre 2001. -
- Codice Amministrazione Digitale, D.Lvo. 7/5/05 n 82, "Codice dell'amministrazione digitale" http://www.parlamento.it/leggi/deleghe/05082dl.htm
- Decreto Legislativo 28 febbraio 2005, n. 42 "Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229" http://www.parlamento.it/leggi/deleghe/05042dl.htm

2.12 SISTEMA INFORMATIVO UNITARIO DELLE AMMINISTRAZIONI PUBBLICHE

L'idea di creare un sistema informativo unitario delle amministrazioni pubbliche si sviluppa su diversi piani e comprende diversi elementi: in particolare:

1. infrastrutture di base;
2. servizi di trasporto ed interoperabilità;
3. gestione integrata delle principali risorse comuni e dei processi condivisi;
4. cooperazione applicativa;
5. reingegnerizzazione dei processi;
6. formazione.

Per quanto riguarda l'informatizzazione di base si sta perseguendo una massiccia acquisizione di nuove tecnologie (stazioni di lavoro, reti locali e server) come la diffusione dei personal computer, nonché il loro completo collegamento in rete per assicurare l'accesso ai servizi della Rete Unitaria.

L'acquisizione dei servizi di trasporto ed interoperabilità della Rete Unitaria costituisce, per molte amministrazioni, una occasione di **ridefinizione delle proprie esigenze**. Tale innovazione porta, sia all'aumento dei siti collegati, sia all'incremento della potenza trasmissiva (anche in vista dell'adozione di servizi avanzati: immagini, videoconferenza, telelavoro, etc...). Si va definendo un nuovo scenario che consenta, a tutte le amministrazioni centrali, di assicurare l'interconnessione dei propri sistemi informativi automatizzati con quelli delle altre amministrazioni (centrali e locali).

2.13 A REINGEGNERIZZAZIONE DEI PROCESSI

La Rete Unitaria comporta una grande trasformazione organizzativa all'interno della Pubblica Amministrazione

REINGEGNERIZZAZIONE DEI PROCESSI

Sviluppare, in modo sistematico, progetti di innovazione organizzativa e ristrutturazione dei processi organizzativi:

- il flusso delle attività di processo;
- la semplificazione e la razionalizzazione delle norme di regolazione del processo;
- l'uso delle tecnologie informatiche.

QUALI SONO LE CONSEGUENZE DELLA RETE UNITARIA?

In realtà l'adozione di una Rete unitaria ha un grande impatto anche sui processi lavorativi all'interno di tutta la P.A. Si aprono nuove possibilità di rapporti intersettoriali e di lavorare in maniera differente.

In poche parole: i progetti di reingegnerizzazione organizzativa, all'interno di un'amministrazione pubblica, coinvolgono gli aspetti giuridici, tecnologici, ed organizzativi.

In particolare con la reingegnerizzazione amministrativa si desidera:

- guidare le risorse coinvolte a formulare il progetto innovativo in modo rigoroso e sistematico: sottolineando le motivazioni di fondo, il nuovo processo organizzativo, la sua giustificazione in termini di crescita di efficacia, efficienza ed economicità. Il metodo deve guidare ad esplicitare i vincoli normativi, gli aspetti organizzativi/tecnologici ed i costi, prima e dopo la proposta innovativa. Esso deve poter essere compreso ed utilizzato, in modo sostanzialmente autonomo, anche da chi non ha competenze tecniche ed ha una cultura di tipo amministrativo;
- accrescere la cultura e quindi promuovere atteggiamenti e conoscenze che consentano di formulare proposte innovative, capirne profondamente il significato ed essere in grado di condividerle;
- raccogliere concreti progetti di riorganizzazione dei processi e degli uffici, per arrivare, eventualmente, ad un disegno elaborato dell'amministrazione.

La reingegnerizzazione dei processi lavorativi all'interno della P.A. comporta una ricomposizione delle attività esistenti, l'automazione di alcune per mezzo dell'informatica, l'introduzione di nuove attività e nuovi prodotti.

1. La semplificazione normativa
2. L'arricchimento del sistema di comunicazione
3. L'introduzione di pratiche di buona informatica

In particolare per:

1. IL MIGLIORAMENTO DELLA COMUNICAZIONE SONO PREVISTI INTERVENTI DEL TIPO:
   - introduzione di attività/prodotti che accrescono la comunicazione; ristrutturazione dei flussi di comunicazione formali ed informali tra le persone, tra gli uffici, con i cittadini, tra amministrazioni diverse, sia per fornire ad ognuno le informazioni necessarie, sia per realizzare la trasparenza dei comportamenti e delle responsabilità di ognuno.
   - eliminazione delle attività e delle unità organizzative, che di fatto ostacolano i processi di comunicazione ed impediscono la trasparenza del sistema
   - introduzione del controllo sociale, del confronto, della trasparenza delle prestazioni e delle responsabilità, per motivare le persone ad assumere comportamenti corretti.

2.L'UTILIZZO DELLA BUONA INFORMATICA PUÒ SINTETIZZARSI IN:

- automazione delle procedure ripetitive:
- la buon'informatica fa crescere efficacia ed efficienza, fa risparmiare sforzi inutili e genera buoni prodotti informativi;
- la cattiva informatica fa fare più fatica e genera prodotti informativi mediocri;
- fornire informazioni:
- la buon'informatica produce informazioni ricche, pregnanti e tempestive;
- la cattiva informatica rende meno accessibile l'informazione, propone informazioni ridondanti, in ritardo, ed impedisce l'accesso a quelle significative;
- creare trasparenza:
- la buon'informatica rende chiaro ad ognuno chi fa che cosa, e quanto bene lo fa;
- la cattiva informatica diminuisce la trasparenza su ruoli e responsabilità;
- creare integrazione organizzativa:
- la buon'informatica accresce il flusso di comunicazione tra uffici, li rende più vicini e più interdipendenti;
- la cattiva informatica isola, allontana gli uffici, frantuma l'organizzazione.

2.14 RETE E AUTONOMIA LOCALE

COME È FATTA LA RETE?

Il suo obiettivo è garantire, a qualunque utente, purché debitamente autorizzato e nel pieno rispetto di stringenti requisiti di sicurezza, di accedere alle procedure ed ai dati utilizzati dalla propria e dalle altre amministrazioni, mediante l'uso di strumenti informatici in grado di scavalcare le diverse tecnologie utilizzate localmente.

La Rete Unitaria è dunque vista come una rete di reti alle cui componenti, comprensive di tutte le risorse software e hardware controllate dalle amministrazioni e denominate domini, **è riconosciuta piena autonomia funzionale ed organizzativa**

Ciò vuol dire che:

Non è richiesto alle singole amministrazioni di adeguarsi a specifiche norme nella realizzazione dei propri sistemi informativi.

E' un concetto molto importante perché significa che con la RUPA non si richiede alle Amministrazioni locali di costruire una Rete standard per tutti con regole e comportamenti stabiliti a priori (cosa che sarebbe difficile realizzare)

LA RETE CONSENTE IL MANTENIMENTO DELL'AUTONOMIA LOCALE!

2.15 E PORTE DELLA RETE

QUALI SONO LE PRINCIPALI VIE DI ACCESSO ALLA RUPA ?

Le principali vie di accesso alla RUPA sono le porte ed in particolare:

i. La porta di rete, è l'unico punto logico di connessione tra le amministrazioni ed il dominio della Rete unitaria
ii. La porta applicativa è il nodo in cui sono disponibili i servizi che ogni dominio vuole esportare.
iii. La porta delegata, è l'elemento architetturale che accede per conto di ciascun utente di un dominio ai servizi esterni

La **porta di rete**, è l'unico punto logico di connessione tra le amministrazioni ed il dominio della Rete unitaria, il quale si compone di una dorsale che veicola il traffico tra le amministrazioni, tra amministrazioni ed enti locali, e verso Internet o altre reti esterne alla P.A.

La **porta applicativa** è il nodo in cui sono disponibili i servizi che ogni dominio vuole esportare. Questo potente meccanismo di astrazione, permette di incapsulare le procedure esistenti, permettendo il loro utilizzo da parte di altre amministrazioni e la creazioni di nuove applicazioni che utilizzano servizi di più amministrazioni.

La **porta delegata**, è l'elemento architetturale che accede per conto di ciascun utente di un dominio ai servizi esterni, permettendo una migliore distribuzione delle responsabilità e delle autorizzazioni.

2.16 RINCIPALI AREE DI INTERVENTO

CIO' VUOL DIRE CHE LE PRINCIPALI AREE DI INTERVENTO SONO

Trasporto

Interoperabilità

Cooperazione applicativa

Le principali aree di intervento della RUPA sono:

- Trasporto, inteso come possibilità di trasmettere messaggi sulla rete, in modo affidabile;
- Interoperabilità, ovvero disponibilità di funzioni di adattamento e conversione, che rendono possibile lo scambio di dati, file, posta elettronica, tra sistemi non omogenei;
- Cooperazione applicativa, cioè capacità delle applicazioni di una amministrazione, di fare uso di servizi messi a disposizione dalle altre.

E' evidente che in questo modo è possibile ottenere miglioramenti significativi:

- sull'efficienza della pubblica amministrazione;
- sui costi organizzativi dei servizi;
- sulla qualità dei servizi ai cittadini ed alle imprese.

2.17 SERVIZI PER IL TRASPORTO

IN CHE MODO LA RUPA GARANTISCE I SERVIZI DI TRASPORTO?

I Servizi trasmissivi di trasporto della RUPA sono:

- Rete privata IP;
- Circuiti virtuali di reti private virtuali;
- Circuiti trasmissivi del tipo CDN.

I servizi per il trasporto consentono alle singole amministrazioni di realizzare le reti geografiche per la connessione di tutti i propri siti e di collegarsi con altre amministrazioni, per poter realizzare i servizi per l'interoperabilità e per la cooperazione applicativa.

2.18 SERVIZI PER LA COOPERAZIONE

IN CHE MODO LA RUPA GARANTISCE I SERVIZI DI INTEROPERABILITA'

Servizi per l'interoperabilità

Questi servizi comprendono:

- Posta elettronica;
- Trasferimento file;
- terminale virtuale;
- Accesso a News, a World Wide Web ed alla rete Internet.

COMPRENDONO CIOÈ I SERVIZI GENERALIZZATI, NECESSARI PER CONSENTIRE LO SCAMBIO DI DATI STRUTTURATI E L'ACCESSO AI SERVIZI APPLICATIVI DELLE DIVERSE AMMINISTRAZIONI.

Essi sono debitamente corredati di servizi di gestione e supporto (DNS, Directory Service, Tempo ufficiale, Call Centre, Formazione); consentono, altresì, in modo sicuro, lo scambio di informazioni tra amministrazioni e, se richiesto, al loro interno.

2.19 SERVIZI PER LA COOPERAZIONE APPLICATIVA

Comprendono i servizi generalizzati, necessari per consentire lo scambio di dati strutturati e l'accesso ai servizi applicativi delle diverse amministrazioni.

Entro il 2010 si prevede la disponibilità dei servizi di cooperazione applicativa e l'evoluzione al servizio IP, all'interno delle reti geografiche delle singole amministrazioni.

2.20 CONDIVIDERE LE INFORMAZIONI

La condivisione delle informazioni e della cooperazione applicativa comporta che:

1. ogni amministrazione porti nel sistema unitario un proprio sistema accessibile in termini tecnologici e funzionali,
2. il sistema sia supportato da una adeguata qualità iniziale e gestionale delle informazioni trattate.

Per questo:

LA REVISIONE DELLA COMPONENTE ORGANIZZATIVA E L'APPRONTAMENTO DELLE NECESSARIE INFRASTRUTTURE TECNOLOGICHE DI BASE SONO DI PARI IMPORTANZA.

Si è realizzata la disponibilità del servizio di trasporto per le reti geografiche delle singole amministrazioni, del servizio di collegamento IP tra amministrazioni e dei servizi per l'interoperabilità tra amministrazioni. Si prevede inoltre l'individuazione e lo sviluppo dei servizi di cooperazione applicativa.

Si è realizzata la disponibilità dei servizi di cooperazione applicativa e l'evoluzione al servizio IP, all'interno delle reti geografiche delle singole amministrazioni.

2.21 L'ORGANIZZAZIONE DEL SERVIZIO

Infrastruttura tecnologica dei servizi d'interoperabilità:

- Utilizzo di regola architettuali standard ed uniformi;
- Tali regole saranno applicate sia nei sistemi che nei dati;
- Permettendo un'implementazione veloce dei cambiamenti ed una facilità di gestione.

La scelta dell'architettura, cioè la scelta della struttura logica e tecnologica della Rete riveste una grande importanza nell'economia complessiva del progetto.

Infatti essa indica il modello di riferimento e le linee guida, a fronte delle quali verificare qualunque ipotesi di modifica e revisione dei componenti del sistema informativo. Inoltre, essa è utilizzata per ricondurre le scelte informatiche, presenti e future, all'interno di una visione strategica unitaria.

2.22 LINEE GUIDA

QUALI SONO LE LINEE GUIDA PRINCIPALI DEL SISTEMA?

Le linee guida principali del sistema che è alla base della RUPA sono:

- Apertura ed aderenza agli standard internazionali
- Utilizzo di tecnologie allo stato dell'arte
- Architettura applicativa Client/Server
- Architettura aperta al mondo WEB
- Espandibilità e scalabilità per future esigenze
- Altissima disponibilità del complesso HW e SW
- Utilizzo di prodotti software standard
- Integrazione comunicativa e gestionale.

Il sistema prevede l'utilizzo di applicativi integrati in cui la Base Dati sia unica e distribuita con un unico insieme di regole di definizione.

Nella fruizione degli applicativi l'utente è garantito da rischi di perdite di dati poiché ogni server ha un backup in grado di dare lo stesso servizio, in caso di **caduta cioè in caso di arresto del sistema.**

I server sono accessibili dalla rete, da qualunque utente, con un'unica modalità d'accesso. Essi seguono gli stessi standard ed assicurano la crescita tecnica, qualora si renda necessaria.

Inoltre: Il sistema di reporting consente, attraverso strumenti generalizzati e di facile utilizzo, l'analisi dei dati, fornendo potenti mezzi per la costruzione di report e di studi analitici in tempo reale sul processo. Ciò permette:

- ai **gestori** di correggere proattivamente eventuali **sbavature** nell'erogazione dei servizi;
- agli **utenti finali** abilitati di conoscere ed analizzare informazioni relative ai servizi erogati.

È garantita sia la sicurezza dagli attacchi esterni, sia l'integrità interna, non solo registrando tutte le operazioni fatte e chi le fa, ma anche implementando metodologie per garantire l'integrità dei file di Log, etc…

2.23 CENTRO TECNICO

CENTRO TECNICO
È un centro di controllo centrale che ha funzioni, tra l'altro, di supervisione dei centri di controllo e gestione (CCG) i quali operano direttamente sulla Rete Unitaria e, di assistenza alle singole Amministrazioni soprattutto su tematiche contrattualistiche (sempre legate alla Rete Unitaria).

Il centro tecnico (CT) ha funzioni, tra l'altro, di supervisione sui Centri di controllo e gestione (CCG) i quali operano direttamente sulla Rete Unitaria, e di assistenza alle singole Amministrazioni soprattutto su tematiche contrattualistiche (sempre legate alla Rete Unitaria).

Il Centro Tecnico, come Unità Organizzativa, in relazione ai Servizi per l'Interoperabilità nel Dominio della Rete Unitaria, assume i compiti di:

- Coordinare, controllare e analizzare le prestazioni ed i livelli di servizio contrattuali erogati dal Fornitore.
- Intraprendere iniziative ritenuta utili al fine di rendere pienamente operativi i Servizi per l'Interoperabilità.
- Coordinare, controllare e analizzare lo stato della sicurezza.

Inoltre supervisiona il funzionamento globale dei servizi erogati dal CG-I, in termini di Accesso al Sistema per il Monitoraggio della Qualità dei Servizi per l'Interoperabilità (attivo presso il CG-I) e Accesso al Sistema di Sicurezza.

2.24 CENTRO DI GESTIONE

Il centro progettato con tecnologie sofisticate, garantisce i livelli di servizio concordati e permette la flessibilità appropriata, fornendo una piattaforma scalabile per il supporto dei requisiti di interoperabilità delle Amministrazioni.

Un attributo estremamente importante del sistema è la sua scalabilità.

I sistemi che fanno capo al Centro di Gestione, supportano con facilità la crescita di ambienti complessi, bilanciando e gestendo un alto volume di transazioni ed analizzando e raccogliendo dati da un gran numero di server.

Il Centro di Gestione ha la funzione di:

- Erogare i Servizi per l'Interoperabilità tra Domini di Amministrazioni differenti (nel rispetto dei livelli di servizio), nei confronti delle Amministrazioni.
- Controllare il corretto funzionamento del servizio di trasporto nel Dominio della Rete unitaria, sia per accessi IP che per i circuiti virtuali.
- Segnalare al Centro Tecnico e sollecitare il superamento da parte del CG-T, malfunzionamenti o un degrado dei livelli di servizio di trasporto nel Dominio della Rete Unitaria.
- Svolgere funzioni di help-desk di primo e di secondo livello, nei confronti del Centro di Gestione dell'Amministrazione, se presente, relativamente ai servizi tra Dominio ed eventualmente per i servizi addizionali, limitatamente ai servizi di hosting, mirroring ed accesso alle banche dati esterne.

2.25 FIGURE INTERESSATE

Il sistema R.U.R.A. prevede dunque la presenza di centri gestori e quindi di alcune figure professionali che presenza di alcune figure specifiche che hanno il compito di gestire i processi e di supportare l'utilizzo della rete:

i gestori del Centro Tecnico

i Gestori del CG-I delle Amministrazioni

I Gestori del Centro Tecnico

Sono coloro che operano quotidianamente presso il Centro Tecnico, l'Unità Organizzativa istituita presso l'Autorità denominata. Il loro compito è quello di:

Coordinare, controllare e analizzare lo stato della sicurezza ed i livelli di servizio.

I prerequisiti richiesti, sono:

- La competenza nel settore dell'informatica distribuita;
- la conoscenza delle problematiche relative a reti di calcolatori ed alla sicurezza dei sistemi distribuiti.

I Gestori del CG-I delle Amministrazioni

Sono coloro che operano quotidianamente nell'Unità Organizzativa istituita presso ogni Amministrazione Centrale, denominata CG-I. Hanno mansioni di:

- Coordinamento, controllo ed analisi dei livelli di servizio contrattuali erogati, svolgendo le funzioni di raccordo tra i servizi di interoperabilità interna al proprio Dominio ed i servizi di interconnessione applicativa del CG-I (DNS di Amministrazione, indirizzamento, etc...)
- Tale ruolo prevede:
- La competenza nel settore dell'informatica distribuita
- La conoscenza delle problematiche relative a reti di calcolatori e delle applicazioni per sistemi distribuiti.

2.26 PIANO TRIENNALE

Il progetto RUPA prevedeva un Piano Territoriale per l'informatica 2000-2002, al fine di acquisire i servizi di collegamento previsti dalla Rete Unitaria.

Questo passaggio organizzativo e culturale avviene in piena coerenza con le linee strategiche della Pubblica Amministrazione, che sono finalizzate a:

- aumentare l'efficienza interna alle amministrazioni per migliorarne i processi, sfruttando le potenzialità della rete unitaria

- porre i cittadini e le imprese al centro della propria missione ed aumentare conseguentemente gli investimenti in software applicativi.

Il prossimo triennio sarà caratterizzato da una nuova focalizzazione orientata ai sistemi applicativi, all'utilizzo produttivo dei servizi informatici ed al miglioramento dei processi e dei risultati. Questi elementi sono sempre stati presenti negli obiettivi e nelle iniziative della Pubblica Amministrazione, ma è evidente che la rinnovata disponibilità delle infrastrutture tecnologiche, accentui l'attualità e la priorità dell'impegno su questi temi.

Il nuovo piano triennale risponde a queste esigenze dando nuovo impulso a progetti di miglioramento nelle principali aree di funzionamento (gestione del personale, gestione del protocollo e dei flussi documentali, utilizzo sicuro dei documenti informatici, nuovo sistema dei pagamenti elettronici, introduzione della nuova contabilità e del controllo di gestione). Il nuovo piano triennale ipotizza inoltre un maggiore utilizzo delle tecnologie dell'informazione e della comunicazione nell'erogazione

dei servizi verso cittadini ed imprese (siti Web, posta elettronica, call center, sistemi integrati per la gestione condivisa delle informazioni di base quali anagrafi, registro imprese etc...). Attraverso queste iniziative è possibile attuare il quadro normativo riguardante l'introduzione del documento e dell'archiviazione elettronica, della firma digitale, del protocollo informatico, del telelavoro.

Si rende, quindi, necessario assicurare concrete possibilità di collegamento **sicuro** tra le **amministrazioni centrali** (organizzate sulla rete unitaria) e gli **enti locali**. Altra necessità è quella di ridisegnare gli attuali sistemi centrali con la distribuzione di funzionalità operative e la realizzazione di adeguati sistemi di governo integrato. In molti casi (Lavoro, Agricoltura, Ambiente, etc..), si tratta di passare, da sistemi informativi a servizio di un Ministero, a veri e propri sistemi di supporto alla pluralità degli attori pubblici coinvolti.

Il sistema informativo unitario delle amministrazioni pubbliche comprende:

1. Lo sviluppo dei principali progetti intersettoriali.
2. Le attività per il completamento e l'avvio operativo delle infrastrutture.
3. La risposta alle problematiche per la gestione dei sistemi distribuiti che si vanno realizzando.

Gli interventi per il necessario consolidamento dei sistemi esistenti.

2.27 PIANO TRIENNALE 2007-2009

Il piano triennale 2007-2009 per l'informatica nella pubblica amministrazione centrale

Fra le principali pubblicazioni che ogni anno fotografano lo stato dell'informatizzazione nella pubblica amministrazione italiana vi è quella redatta dal Cnipa. Quest'anno il documento ha impostato un piano triennale per il 2007-2009 in cui sono specificate le strategie comuni che le varie amministrazioni dovranno seguire nella gestione della spesa informatica e nell'implementazione tecnologica degli iter burocratici. Il documento è stato

redatto tenendo conto delle proposte inviate dalle amministrazioni centrali e, per ogni suggerimento, è stata verificata la coerenza con le linee strategiche

elaborate dal Cnipa stesso in base al quadro di indirizzo stabilito dal Ministero per le Riforme e le Innovazioni nella Pa.

Per il triennio 2007-2009 sono state in particolare utilizzate le proposte di 19 amministrazioni centrali dello Stato (tutti i Ministeri, la Presidenza del Consiglio, l'Avvocatura generale dello Stato, il Consiglio di Stato, la Corte dei conti e la Scuola Superiore della Pubblica Amministrazione) e di 12 enti pubblici non economici. Il piano triennale rappresenta quindi un documento preliminare ed estremamente dettagliato, che è fondamentale nella valutazione complessiva della programmazione finanziaria.

Il documento espone l'analisi dei fabbisogni finanziari per l'acquisizione di beni e servizi Ict da parte della pa centrale nell'arco del triennio, ed evidenzia come sono stati programmati attività e progetti di innovazione tecnologica. Per ognuno dei tre anni sono stati stabiliti specifici obiettivi e spese. Particolare attenzione è stata data ai capitoli di spesa del primo anno in cui vengono definite le singole linee strategiche. Nel primo anno si stima il fabbisogno, ripartito normalmente fra le spese finanziate dalla disponibilità di bilancio ordinario e quanto invece necessita di un intervento straordinario.

La spesa complessiva di tutte le amministrazioni presenti nel piano è stato stimato in circa 2,25 miliardi di euro per il 2007, di 2 per il 2008 e di 1,86 per il 2009. In totale 6,2 miliardi di euro per tutto il triennio. Per le sole amministrazioni centrali dello Stato si spenderanno per il triennio 4,8 miliardi di euro, di cui 4,7 per le esigenze ministeriali. Per gli enti pubblici non economici invece il fabbisogno triennale sarà pari a 1,36 miliardi di euro.

Le linee strategiche per l'informatizzazione della pubblica amministrazione dovranno nell'immediato confrontarsi con i tagli di bilancio apportati dalla legge finanziaria agli stanziamenti dedicati all'informatica di servizio. La riduzione di stanziamenti è stata notevole rispetto alle proposte formulate nel piano precedente, quello 2006-2008. Una differenza che ridurrà fortemente gli investimenti e che si colloca in un contesto in cui comunque cresce l'esigenza di servizi efficienti e telematici da parte della Pa.

Per questo motivo, le linee strategiche elaborate dal Cnipa saranno di tipo strutturale e a lungo periodo. Fondamentale sarà la razionalizzazione degli investimenti che saranno fatti sulle tecnologie disponibili, eliminando duplicazioni e accelerando l'adozione di tecnologie innovative.

Il piano specifica anche quali saranno le iniziative principali da seguire per accelerare l'informatizzazione della pubblica amministrazione. Fra queste vi è l'attuazione delle indicazioni fornite nel Codice dell'Amministrazione Digitale, che è stato istituito appositamente per semplificare il sistema giuridico di riferimento. Il Codice introduce il 2 diritto per il cittadino di dialogare con la PA attraverso le nuove tecnologie ed il dovere, per le amministrazioni, di rendere disponibile le informazioni anche in formato digitale.

Nei prossimi anni l'attuazione del Codice richiederà alle Pa di attuare alcune importanti innovazioni quali:

- la messa a disposizione dei cittadini degli indirizzi di posta elettronica degli uffici competenti agli atti di maggiore interesse;

- l'utilizzo della posta elettronica come mezzo di comunicazione e trasmissione documenti;
- l'adozione della Carta Nazionale dei Servizi (CNS), come strumento per accedere in sicurezza ai servizi di rete;
- l'adozione di misure di sicurezza per garantire riservatezza e integrità dei dati;
- l'introduzione di un "centro di competenza" interno ad ogni pubblica amministrazione.

Questi sono alcuni dei principali servizi che dovranno essere attuati per razionalizzare le applicazioni informatiche. A queste indicazioni si aggiunge un adeguamento tecnico economico per quel che riguarda la Rete unitaria della Pubblica amministrazione (RUPA) che, come è previsto anche nelle linee strategiche 2006-2008, dovrà transitare sul Sistema pubblico di connettività (SPC). Sul versante del SPC è anche previsto, dal primo semestre 2007, l'avvio di alcuni nuovi servizi che integreranno quelli forniti dal RUPA e permetteranno una forte interoperabilità e cooperazione applicativa.

Fra questi vi saranno sistemi di **messagistica evoluta, posta certificata, servizi di help desk informatico e di sicurezza applicativa.**

Il Cnipa dovrà intervenire apportando notevoli innovazioni in molti settori. Oltre a migliorare il software della pa, che permetterà un notevole risparmio di risorse, il Cnipa si concentrerà su servizi innovativi per cittadini e imprese. Fra questi l'm-Government per cui il Cnipa istituirà un apposito Centro servizi mobile con l'obiettivo di costituire una piattaforma unitaria da cui erogare appositi servizi. Si potrà accedere alla piattaforma attraverso un numero unico che permetterà un risparmio sino a 32 milioni d euro l'anno rispetto a servizi erogati attraverso differenti canali di comunicazione.

Il Cnipa continuerà inoltre ad operare sul versante dell'open source, favorendo da un lato l'ascolto delle esigenze delle pa, grazie all'osservatorio che è stato costituito, e dall'altra diffondendo la cultura e la conoscenza dei vantaggi disponibili utilizzando questo tipo di strumenti.

Infine il Cnipa opererà per sviluppare ed implementare, con nuovi servizi, i portali che sono stati appositamente creati per cittadini e imprese. Fra questi vi è il portale del cittadino (italia.gov.it) che verrà ristrutturato con una nuova architettura e con nuove informazioni e il portale per le imprese (impresa.gov.it) che includerà il registro informatico degli adempimenti amministrativi per le imprese. Il registro sarà utilizzato come banca dati certificata di riferimento per definire, in collaborazione con le associazioni di categoria, adempimenti omogenei al risultato atteso dall'impresa.

In informatica, **open source** (termine inglese che significa *sorgente aperto*) indica un software i cui autori (più precisamente i detentori dei diritti) ne permettono, anzi ne favoriscono il libero studio e l'apporto di modifiche da parte di altri programmatori indipendenti. Questo è realizzato mediante l'applicazione di apposite licenze d'uso.

La collaborazione di più parti (in genere libera e spontanea) permette al prodotto finale di raggiungere una complessità maggiore di quanto potrebbe

ottenere un singolo gruppo di lavoro. L'open source ha tratto grande beneficio da Internet, perché esso permette a programmatori geograficamente distanti di coordinarsi e lavorare allo stesso progetto. (Wikipedia)

2.28 POSTA CERTIFICATA

L'e-mail e la Posta Elettronica Certificata

L'e-mail è ormai lo strumento di comunicazione elettronica più utilizzato per lo scambio di comunicazioni. La posta elettronica o e-mail (acronimo di Electronic Mail) è un mezzo di comunicazione in forma scritta via Internet. Il principale vantaggio dell'e-mail è l'immediatezza. I messaggi possono includere testo, immagini, audio, video o qualsiasi tipo di file. 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 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 gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

DPR 11 febbraio 2005 che disciplina l'utilizzo della PEC

Il DPR 11 febbraio 2005, n. 68 (G.U. 28 aprile 2005, n. 97) (PDF) disciplina le modalità di utilizzo della Posta Elettronica Certificata (PEC) non solo nei rapporti con la PA, ma anche tra privati cittadini. In sintesi le novità contenute nel provvedimento:

- nella catena di trasmissione potranno scambiarsi le e-mail certificate sia i privati, sia le PA. Saranno i gestori del servizio (art. 14), iscritti in apposito elenco tenuto dal Cnipa (che verificherà i requisiti soggettivi ed oggettivi inerenti ad esempio alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo), a fare da garanti dell'avvenuta consegna.
- per iscriversi nell'elenco dovranno possedere un capitale sociale minimo non inferiore a un milione di euro e presentare una polizza assicurativa contro i rischi derivanti dall'attività di gestore;
- messaggi verranno sottoscritti automaticamente da parte dei gestori con firme elettroniche. Tali firme sono apposte su tutte le tipologie di messaggi PEC ed in particolare sulle buste di trasporto e sulle ricevute per assicurare l'integrità e l'autenticità del messaggio;
- i tempi di conservazione: i gestori dovranno conservare traccia delle operazioni per 30 mesi;

- i virus: i gestori sono tenuti a verificare l'eventuale presenza di virus nelle e-mail ed informare in caso positivo il mittente, bloccandone la trasmissione (art. 12);
- le imprese, nei rapporti intercorrenti, potranno dichiarare l'esplicita volontà di accettare l'invio di PEC mediante indicazione nell'atto di iscrizione delle imprese.

2.29 ROTOCOLLO INFORMATICO

Gestione del protocollo informatico, dei documenti e dell'archivio

Il legislatore definisce **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; il protocollo informatico si colloca all'interno del sistema come infrastruttura di base destinata ad avviare concretamente il processo di ammodernamento della pubblica amministrazione. Ogni sistema di protocollo informatico deve ottemperare alle specifiche indicazioni riportate nel DPR 445-28/12/2000 e nel regolamento attuativo DPCM 31/10/200.

L'attuale quadro normativo e regolamentare in materia di gestione informatica del protocollo, dei documenti e degli archivi, favorisce l'innovazione e il miglioramento dei servizi della Pubblica Amministrazione in termini di **efficienza, efficacia, economicità e trasparenza dell'azione amministrativa** a favore dei cittadini e delle imprese. In questo ambito il CNIPA svolge funzioni di indirizzo e di coordinamento alle amministrazioni in termini di:

- assistenza e consulenza per favorire la diffusione del sistemi di protocollo informatico e gestione documentale;
- azioni di sensibilizzazione e comunicazione;
- rilevazione periodica dello stato di attuazione delle normativa;
- attività di supporto alle amministrazioni secondo un principio di sussidiarietà attraverso l'erogazione di un servizio di gestione del protocollo informatico e dei flussi documentali in modalità ASP, peraltro riconosciuto come uno delle 100 migliori iniziative pubbliche dal Ministro per la pubblica amministrazione e l'innovazione.

Approfondimento:
http://www.pubblica.istruzione.it/amministrazione/progetto.shtml

2.30 FIRMA DIGITALE

La **firma digitale**, o firma elettronica qualificata, basata sulla tecnologia della crittografia a chiavi asimmetriche, è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta. La firma digitale è un sistema di autenticazione forte in quanto si basa sull'uso di un certificato digitale memorizzato su di un dispositivo hardware. I certificati su cui si basa possono essere più di uno.

Un tipico schema di firma digitale consiste di tre algoritmi:

1. un algoritmo per la generazione della chiave G che produce una coppia di chiavi (*PK*, *SK*). *PK* è la chiave pubblica di verifica della firma (Public

Key) mentre *SK* è la chiave privata (Secret Key) posseduta dal firmatario, utilizzata per firmare il documento.
2. un algoritmo di firma S che, presi in input un messaggio *m* ed una chiave privata *SK* produce una firma σ.
3. un algoritmo di verifica V che, presi in input il messaggio *m*, la chiave pubblica *PK* e una firma σ, accetta o rifiuta la firma. (Wikipedia).

3. La sicurezza informatica

3.1 IL FATTORE SICUREZZA

Nella gestione ed utilizzo di un sistema informativo, è di fondamentale importanza tenere sotto controllo costante il fattore sicurezza.

Un primo è quello di stabilire il programma della sicurezza formalizzando l'attenzione sulla gestione e sulla struttura del programma stesso in maniera da ottenere:

- la misurazione del rischio
- la mitigazione del rischio attraverso la selezione di controlli efficaci e di costo ragionevole.

Gli aspetti organizzativi e attività relative alla sicurezza dei computer riguardano:

- Politica di sicurezza dei computer e dell'informazione;
- Gestione e struttura del programma di sicurezza;
- Gestione del rischio;
- Sicurezza nel ciclo di vita di un sistema informatico;

Affidabilità.

PARTICOLARE IMPORTANZA HA L'AFFIDABILITÀ CHE RAPPRESENTA IL GRADO DI FIDUCIA CHE SI HA NEL CORRETTO FUNZIONAMENTO DELLE MISURE DI SICUREZZA.

E' SEMPRE ATTRAVERSO LA GESTIONE DEL RISCHIO CHE SI GARANTISCE L'AFFIDABILITÀ DI UN SISTEMA DI SICUREZZA.

3.2 INTERVENTI

In caso di danni o malfunzionamento al sistema è necessario intervenire per:

1. recuperare i dati
2. identificare il responsabile
3. identificare i metodi utilizzati
4. revisionare la documentazione
5. per poter intervenire tempestivamente sono necessari una normativa sulla sicurezza dei computer e una serie di strumenti messi a disposizione della tecnologia.

In caso di problemi è bene seguire procedure codificate.

VEDIAMO ALCUNE RACCOMANDAZIONI DI CARATTERE GENERALE:

1. recuperare o ripristinare i beni sottratti o danneggiati a causa di un attacco interno od esterno;
2. identificare il responsabile dell'attacco;

3. identificare i metodi utilizzati dall'intruso per rompere la sicurezza in modo da prevenire
4. che l'attacco si verifichi una seconda volta;
5. revisionare la documentazione e la registrazione di tutte le attività per trovare le prove e le tracce di un attacco.

3.3 RISCHI

PERCHÈ È NECESSARIA LA SICUREZZA?

1. Per la progressiva diffusione degli strumenti informatici e telematici all'interno delle organizzazioni;
2. per limitare i rischi di un coinvolgimento sia patrimoniale che penale (in relazione all'uso o all'abuso degli strumenti)
3. per individuare e adottare contromisure adeguate sul piano organizzativo e tecnico.

COME CI SI DEVE COMPORTARE IN CASO DI ABUSI DA PARTE DEL PERSONALE DELL'ORGANIZZAZIONE?

È doveroso segnalare che gli abusi degli strumenti informatici, da parte del personale dell'organizzazione, i cui effetti incidano solo su aspetti interni all'organizzazione e non comportino responsabilità verso l'esterno (ad esempio l'uso dei mezzi informatici per scopi diversi da quelli lavorativi: computer game, svolgimento di attività privata in ore lavorative, danneggiamento o distruzione di dati aziendali che non abbiano rilevanza in termini di responsabilità esterna), sono sicuramente non trascurabili, ma esulano dall'analisi dei profili di responsabilità penale e civile dell'organizzazione e della sua dirigenza. Comunque tali problemi possono essere affrontati a livello organizzativo e tecnico.

3.4 SISTEMA INFORMATIVO SICURO

QUALI SONO I REQUISITI PER UN SISTEMA INFORMATICO SICURO?

1. **Disponibilità**: l'informazione ed i servizi che eroga, devono essere a disposizione degli utenti del sistema, compatibilmente con i livelli di servizio;
2. **Integrità**: l'informazione ed i servizi erogati possono essere creati, modificati o cancellati, solo dalle persone autorizzate a svolgere tale operazione;
3. **Autenticità**: garanzia e certificazione della provenienza dei dati;
4. **Confidenzialità** o riservatezza: l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

COME SI FA A VALUTARE IL LIVELLO DI SICUREZZA INFORMATICA?

Per valutare in maniera globale la sicurezza è necessario stimare gli aspetti tecnici (sicurezza fisica e logica), strategici (obiettivi e budget), organizzativi (definizione di ruoli, procedure, formazione), economici (analisi dei costi) ed infine legali (leggi e raccomandazioni, normative).

Si rende quindi necessario, inizialmente, verificare che:

Tutti i componenti, HW e SW, siano fail safe, cioè che ogni loro malfunzionamento o messa fuori operazione non comporti una diminuzione della sicurezza di esercizio, eventualmente anche attraverso una messa fuori uso della particolare stazione interessata.

Le responsabilità dell'esercizio e dei controlli interni di sicurezza siano affidate a persone distinte e collocate nella struttura organizzativa, affinché in alcun modo il responsabile dell'esercizio possa influire sulla carriera/retribuzione del responsabile dei controlli interni di sicurezza.

Le procedure per l'accertamento della qualità delle verifiche, effettuate dal responsabile dei controlli interni di sicurezza sull'operato del team di gestione, siano adeguate.

Sia sempre possibile individuare inequivocabilmente, in un apposito activity log file, l'autore di una qualsiasi operazione.

Sia garantita, al di là di ogni dubbio, l'integrità di questo log file e la sua disponibilità nel tempo per il periodo concordato.

Sia sempre possibile ripristinare il sistema, di fronte a guasti o eventi naturali o dolosi, allo stato in cui si trovava prima del verificarsi dell'evento stesso, in un certo periodo di tempo concordato a priori tra le parti.

Sia garantita l'integrità del SW ad ogni livello, dal sistema operativo alle applicazioni, e dei relativi file di configurazione.

Sia efficace il programma dei test di penetrazione, sia interna che esterna, effettuati periodicamente rispettando la frequenza concordata.

Siano adeguate le procedure per l'effettuazione delle varie operazioni di manutenzione e per il trattamento dei supporti di memorizzazione di massa obsoleti.

Sia valido il programma di accertamento della qualità dei controlli sull'aggiornamento continuo dell'HW e del SW, dal controllo della completa sincronizzazione delle versioni, aggiornate tempestivamente dello stesso SW, all'aggiornamento delle varie patches distribuite dai fornitori per chiudere i vari buchi, mano mano che vengono scoperti.

Patches, un sistema sicuro è un sistema aggiornato!

La produzione di software, commerciale o libera, è usualmente soggetta ad errori di scrittura del codice e malfunzionamenti, chiamati *bug*, che vengono scoperti successivamente al rilascio del software stesso.

Nel suo significato primario, *patch* (letteralmente "pezza") è un termine inglese che in informatica indica, come *hot fix*, un file eseguibile creato per risolvere uno specifico errore di programmazione, che impedisce il corretto funzionamento di un programma o di un sistema operativo. Tali file generalmente vengono rilasciati dagli stessi produttori, nell'attesa di pubblicare una nuova versione del software stesso. (Wikipedia)

3.5 NORMATIVA E SICUREZZA

È OBBLIGATORIO ADOTTARE MISURE DI SICUREZZA?

Una serie di leggi emanate in questi ultimi anni obbligano i fornitori e

gli utenti di servizi informatizzati al rispetto di alcune regole e alla messa in opera di una serie di contromisure finalizzate a prevenire o minimizzare i rischi di un incidente informatico

OGGI L'ADOZIONE DI TALI CONTROMISURE NON È PIU' LASCIATA ALLA DISCREZIONE DELLE SINGOLE AMMINISTRAZIONI MA IN MOLTI CASI È UN OBBLIGO DI LEGGE.

A proposito di Sicurezza dei Sistemi informativi la normativa esistente fornisce indicazione su come affrontare le problematiche della Sicurezza dei Sistemi informativi automatizzati e anche su come realizzare e gestire adeguate misure di protezione.

Tale normativa ha l'obiettivo di:

- incrementare la consapevolezza di rischi e insidie, che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati;
- indicare possibili percorsi tecnici ed organizzativi di salvaguardia per prevenire situazioni di pericolo per le risorse e per chi se ne avvale, nonché per affrontare e risolvere eventuali problemi insorgenti al verificarsi di eventi lesivi del patrimonio informativo;
- supportare la creazione, nell'ambito delle Amministrazioni Pubbliche, di strutture in grado di disegnare, pianificare, implementare e gestire misure di protezione corrispondenti alle esigenze degli specifici contesti di competenza;
- Incrementare l'utilizzo delle risorse informative disponibili su supporto informatico ed accessibili per via telematica con le imprescindibili garanzie di sicurezza;
- chiarire dal punto di vista normativo gli obblighi delle Amministrazioni in merito all'adozione di misure di sicurezza.

3.6 PRINCIPALI NORMATIVE

La legislazione italiana relativa alla sicurezza informatica poggia su tre leggi fondamentali che in questo contesto possono costituire il riferimento normativo:

D lgs n. 518 del 1992, che modifica il regio decreto n.633 del 1941, relativo al diritto d'autore, integrando con norme relative alla tutela giuridica dei programmi per elaboratore.

Legge n. 547 del 1993, che modifica il codice penale italiano introducendo i cosiddetti Computers Crimes.

Legge n. 675 del 1996, che disciplina il trattamento dei dati personali.

D.L.vo 193/2006 meglio conosciuto come Testo Unico sulla Privacy.

La **legislazione sulla privacy** in Italia è attualmente contenuta nel Decreto legislativo 30 giugno 2003, n. 196, intitolato **Codice in materia di protezione dei dati personali e noto anche come Testo unico sulla privacy**.

Il D.Lgs 196/2003 abroga la precedente legge 675/96, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, che era stata introdotta per rispettare gli Accordi di Schengen ed era entrata in vigore nel maggio 1997. Con il tempo a tale norma si erano affiancate ulteriori diverse disposizioni, riguardanti singoli specifici aspetti del trattamento dei dati, che sono state riassunte nel Testo Unico vigente, entrato in vigore il 1º gennaio 2004.

Sull'applicazione della normativa vigila l'Autorità Garante per la protezione dei dati personali, istituita dalla L. 675/1996, e confermata dal Testo Unico del 2003.

L'allegato B del Decreto legislativo 30 giugno 2003, n. 196, prevede il **DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA** (Artt. da 33 a 36 del codice), che definisce misure minime quel complesso di

misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione normativamente richiesto rispetto ai rischi individuati.

3.7 PIANO DELLA SICUREZZA

Per realizzare un sistema di sicurezza informatico efficace ed efficiente si rende necessario disegnare, pianificare, implementare e gestire opportune contromisure.

Tali contromisure saranno di natura

- FISICA
- LOGICA

SI RENDE CIOÈ NECESSARIO ADOTTARE E UTILIZZARE UN VERO E PROPRIO PIANO AZIENDALE CHE TENGA CONTO DI TUTTI I FATTORI CHE POSSONO INFLUIRE SULLA RICUREZZA INFORMATICA

COME SI DEVE FARE METTERE IN SICUREZZA UN SISTEMA INFORMATIVO?

PER FARLO E' NECESSARIO ANALIZZARE ALCUNI FATTORI DETERMINANTI I PIU' IMPORTANTI DEI QUALI SONO:

- Analisi dei rischi
- Definizione delle Politiche di Sicurezza
- Gestione del Rischio
- Il Piano Operativo
- Sicurezza fisica e logica
- Controllo degli accessi antivirus
- Controllo del software
- Riservatezza e autenticità dei dati
- Autenticazione e non ripudio
- Sicurezza organizzativa.

3.8 ANALISI DEI RISCHI

Per definire un piano di sicurezza il primo passo consiste nell'analizzare i rischi presenti, cioè:

1. individuare gli elementi del sistema informativo automatizzato da proteggere;
2. individuare le minacce.

Occorre cioè individuare tutte quelle possibili componenti che hanno un impatto con il problema sicurezza ed analizzare le relazioni che ciascuna di esse ha con le altre e con il resto dell'ambiente esterno.

LA PRIMA COSA DA FARE E' STIMARE E VALUTARE IL RISCHIO INFORMATICO. PER QUESTO MOTIVO IL PUNTO DI PARTENZA E' SEMPRE L'ANALISI DEI RISCHI È LA FASE DI PARTENZA.

CIÒ VUOL DIRE CHE E' NECESSARIO:

1. individuare gli elementi del sistema informativo automatizzato da proteggere e individuare da quali minacce proteggere tali elementi.
2. elencare tutte le possibili componenti che hanno un impatto con il problema sicurezza ed analizzare le relazioni che le singole

componenti hanno fra loro e con il resto dell'ambiente, definendo così un disegno completo del Sistema Informatico.

3. determinare quale sia il patrimonio informativo, in termini di dati e risorse elaborative, oggetto del Piano della Sicurezza.

VEDIAMO NEL DETTAGLIO QUALI SONO GLI ASPETTI PRINCIPALI DA ANALIZZARE:

Risorse Hardware

Rientrano in questa categoria le CPU, terminali, workstation, personal computer, stampanti, disk drive, linee di comunicazione, server, router. Le principali minacce cui questi dispositivi vengono sottoposti sono:

- mal funzionamenti dovuti a guasti o sabotaggi;
- mal funzionamenti dovuti a eventi naturali quali allagamenti e incendi;
- furti e intercettazione.

Quest'ultima minaccia interessa gli apparati di rete, cioè le linee di comunicazione, i router ed i server. È infatti possibile, effettuare il monitoraggio indebito o l' alterazione della trasmissione di dati effettuata da questi apparati, che questa avvenga tra terminali, o tra computer, o tra stazioni di lavoro periferiche e sistemi centrali di elaborazione. Un altro caso può riguardare i video dei quali si possono intercettare le onde elettromagnetiche emesse, per ricostruirne remotamente l'immagine.

Risorse Software

Rientrano in questa categoria, i Sistemi Operativi e Software di Base (utility, diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, i programmi in formato sorgente e oggetto.

Le minacce principali legate all'uso di questi prodotti sono i seguenti.

- La presenza di errori involontari, commessi in fase di progettazione e/o implementazione, che permettono, ad utenti non autorizzati, l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti.
- La presenza di codice malizioso, inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema o per danneggiare lo stesso. Rientrano in questa categoria di minacce i virus, i trojan horse, le bombe logiche, le backdoor.
- Attacchi di tipo denial of service portati a servizi di rete, ma facilmente estendibili a un qualunque servizio. Si tratta di attacchi non distruttivi, il cui obiettivo è saturare la capacità di risposta di un servizio con l'obiettivo ultimo di renderlo inutilizzabile agli altri utenti del sistema.
- I formati sorgente delle applicazioni hanno una certa importanza in quanto possono essere oggetto di furto, sia per un'eventuale rivendita ad altre organizzazioni sia per l'inserimento di codice malizioso.

Dati

Ci si riferisce al contenuto degli archivi, delle Basi di dati, dati di transito, copie storiche, file di log, etc...

Le debolezze dei sistemi operativi e delle applicazioni che operano sulle macchine su cui risiedono, possono costituire una minaccia riconducibili a due tipologie:

1. L'accesso non autorizzato, cioè la possibilità per utenti esterni o interni di visualizzare informazioni riservate a particolari categorie di utenti.
2. Modifiche deliberate o accidentali (la possibilità per utenti non autorizzati di modificare o cancellare dati a loro non appartenenti, errori commessi da utenti autorizzati, che inavvertitamente modificano o cancellano informazioni significative).

Le Risorse Professionali

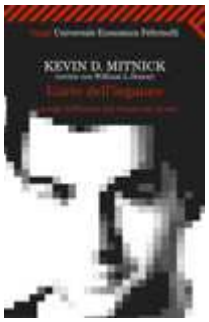
S'intendono gli amministratori di sistemi, i sistemisti, i programmatori, gli operatori, gli utenti finali, i manutentori hardware e software, i consulenti, etc...

È UNA CATEGORIA CHE PUÒ ESSERE OGGETTO DI MINACCE, COMPROMETTENTI LA SICUREZZA DEL SISTEMA, MA PUÒ A SUA VOLTA COSTITUIRE UNA MINACCIA PER LA SICUREZZA DEL SISTEMA.

Nel primo caso, il personale può essere oggetto di attacchi, cosiddetti di **social engineering**, in cui estranei cercano, attraverso varie condotte, di ottenere informazioni utili ad attaccare il sistema (quali le password degli utenti, il contenuto dei file di configurazione, gli indirizzi IP delle macchine e così via).

Nel secondo caso, quando il personale ha una scarsa consapevolezza del problema sicurezza.

Social engineering



Un volume importante che tutti gli amministratori e i responsabili di reti e dati 8sensibili e non) dovrebbero leggere è L'arte dell'inganno I consigli dell'hacker più famoso del mondo di Kevin D. Mitnick edito da Feltrinelli.

Questo libro descrive le strategie di "social engineering" impiegate dagli hacker, dagli agenti dello spionaggio industriale e dai criminali comuni per penetrare nelle reti. Si tratta di tecniche dell'"inganno", di espedienti per usare la buona fede, l'ingenuità o l'inesperienza delle persone che hanno accesso alle informazioni "sensibili".

Documentazioni Cartacee

Le principali minacce cui è sottoposta la documentazione relativa ai programmi, all'hardware, ai sistemi, alle procedure di gestione, etc…, sono la distruzione e/o l'alterazione, ad opera di eventi naturali, o di azioni accidentali, o di comportamenti intenzionali.

Supporti di memorizzazione

Sono i supporti su cui sono tenute le copie dei sw installati, le copie dei file di log e dei back-up. Le principali minacce a tali dispositivi, oltre a quelle già menzionate per i dispositivi cartacei, sono:

- il deterioramento nel tempo;
- l'inaffidabilità del mezzo fisico che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo;
- l'evoluzione tecnologica e del mercato.

Classificazione dei beni e loro valutazione

Ai fini della sicurezza è fondamentale procedere alla classificazione dei beni in funzione degli elementi di integrità, riservatezza e disponibilità. Tale classificazione consentirà di attribuire, ai diversi beni, un valore in funzione di una serie di scenari di impatto significativi ai fini della sicurezza.

La valutazione dei beni è indispensabile per capire la strategicità degli stessi all'interno del Sistema Informativo e per poter quindi, successivamente, valutare il livello di esposizione al rischio.

Sono disponibili diverse metodologie di valutazione dei beni, alcune basate su principi quantitativi (costo di ripristino, costi per elaborazione tramite risorse alternative,..), altre basate su principi qualitativi (perdita di immagine, violazione di assetti legislativi, perdita di efficacia/efficienza nell'operatività,…). È opportuno che la metodologia prescelta consenta di valutare tutti i possibili scenari di impatto che caratterizzano il patrimonio informativo dell'amministrazione, e di effettuare valutazioni che tengano in considerazione sia gli impatti quantitativi che quelli qualitativi.

Nel caso dei Sistemi della P.A. il criterio puramente economico dovrà essere bilanciato da altre valutazioni, più pertinenti al ruolo della P.A. stessa.

I criteri per la valorizzazione, in linea di massima, dovranno tenere conto, in ordine decrescente, di parametri quali:

1. Rischio per la sicurezza dello stato e/o dei cittadini;
2. Interruzione di pubblico servizio;
3. Alterazione di pubblico servizio;
4. Sottrazione ed alienazione di patrimonio pubblico;
5. Danneggiamento di patrimonio pubblico.

Valutazione delle Minacce e delle Vulnerabilità dei beni

L'individuazione delle minacce e delle vulnerabilità cui sono esposti i beni del patrimonio informativo è fondamentale per valutare successivamente l'esposizione al rischio. La valutazione delle minacce e delle vulnerabilità prende in considerazione molte tipologie di potenziali problemi, ognuna delle quali può interessare differenti parti del sistema.

Le categorie delle minacce, possono essere raggruppate nelle seguenti aree:

1. penetrazione logica;
2. penetrazione nelle reti di comunicazione;
3. guasti tecnici delle apparecchiature;
4. errori umani;
5. minacce fisiche.

L'ANALISI DEI RISCHI SI CONCLUDE CON L'INDIVIDUAZIONE DI UN INSIEME DI POSSIBILI CONTROMISURE DI NATURA FISICA, LOGICA ED ORGANIZZATIVA CHE POTREBBERO ESSERE ADOTTATE AL FINE DI ABBATTERE L'ENTITÀ DEL RISCHIO PRECEDENTEMENTE INDIVIDUATA PER CIASCUNA COMPONENTE DEL SISTEMA INFORMATIVO AUTOMATIZZATO E PER CIASCUNA DELLE MINACCE CUI È SOTTOPOSTO, IL LIVELLO DI RISCHIO CHE SI POTREBBE RITENERE ACCETTABILE.

La definizione delle contromisure da attuare dovrebbe considerare per ciascuna minaccia:

1. vulnerabilità;
2. danno potenziale;
3. probabilità dell'evento;
4. rischio per l'Amministrazione;
5. costo di ripristino;
6. priorità nell'implementazione dei meccanismi di sicurezza;
7. contromisure urgenti, ordinarie, future.

PERCHE' E' NECESSARIO DEFINIRE
LE POLITICHE AZIENDALI PER LA SICUREZZA?
Definire le Politiche di Sicurezza Aziendale serve per l'individuazione di criteri generali necessari al raggiungimento di standard soddisfacenti basati sulla nozione di rischio e indipendenti dalla tecnologia correntemente in uso.
LE POLITICHE DELLA SICUREZZA RAPPRESENTANO DELLE LINEE GUIDA ALLE QUALI CIASCUNO DEVE ATTENERSI E STABILISCONO I CRITERI DI COMPORTAMENTO AI QUALI ADEGUARSI.

3.9 POLITICHE DELLA SICUREZZA

POLITICHE DELLA SICUREZZA

La sicurezza deve essere considerata da tutti i dipendenti, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni (uso improprio o distruzione). Le Politiche della sicurezza devono comprendere i seguenti aspetti:

1. **Classificazione delle informazioni**: le informazioni, in qualsiasi forma esse si presentino (posta elettronica, archivi informatici, programmi, etc..), devono essere protette con normative e misure tecniche, commisurate sia all'importanza che esse rappresentano per l'Amministrazione (riservatezza, criticità etc.), sia a specifici requisiti.
2. **Protezione fisica delle risorse**: l'obiettivo è la definizione di misure di sicurezza per la predisposizione e il mantenimento di un ambiente di lavoro protetto che impedisca perdite di informazioni e di patrimonio intellettuale di proprietà. Tale obiettivo è raggiungibile attraverso misure di controllo crescenti, correlate ai rischi ed al valore dei beni e delle informazioni presenti nell'ambiente.
3. **Protezione logica delle informazioni**: anche le misure di sicurezza logica dovranno essere commisurate al livello di classificazione delle informazioni. Ne fanno parte i seguenti aspetti:
    1. il controllo degli accessi alle informazioni;
    2. il mantenimento della loro integrità e riservatezza;
    3. la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno, via Internet, con altre Amministrazioni;

4. la sicurezza delle stazioni di lavoro e dei personal computer;
5. la sicurezza nel processo di sviluppo delle applicazioni informatiche;
6. la sicurezza nella gestione operativa delle installazioni informatiche;
7. la tempestiva rilevazione di eventuali incidenti di sicurezza.

4. **Norme per il Personale**: tutti i dipendenti concorrono alla realizzazione della Sicurezza, pertanto dovranno proteggere le informazioni assegnate loro, per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito dalle Politiche almeno in termini di:
   1. utilizzo delle risorse informatiche;
   2. accesso ai sistemi e ai dati;
   3. uso della password.
5. **Piano di Continuità Operativa**: l'obiettivo è quello di GARANTIRE LA CONTINUITÀ DEL SERVIZIO INFORMATICO e la disponibilità delle informazioni (aggiornate), evitando o limitando i danni al patrimonio informativo, a fronte di una emergenza. A tale scopo ogni Amministrazione ha previsto un Piano di Ripristino delle informazioni e delle operazioni, contenente gli aspetti organizzativi e normativi, le modalità e le risorse di backup necessarie (centro di calcolo, risorse hardware, software, personale etc..) alla ripresa delle attività, a seguito di una emergenza che impedisca la normale erogazione del servizio informatico.
6. **Gestione degli incidenti**: i rischi informatici devono essere costantemente controllati e monitoritati. Inoltre devono essere definite le responsabilità e le modalità con cui gestire eventuali incidenti di sicurezza.
7. **Sviluppo e manutenzione dei sistemi hardware e software utilizzati nel realizzare il piano di Sicurezza**: occorre regolare le procedure con cui il software deve essere aggiornato e/o modificato e gli apparati sostituiti o riparati.

L'APPLICAZIONE DELLE POLITICHE DI SICUREZZA ALL'INTERNO DELL'AMMINISTRAZIONE RICHIEDE LA DEFINIZIONE DI UN INSIEME DI REGOLE CHE FANNO RIFERIMENTO ALLE TECNOLOGIE USATE, ALLE METODOLOGIE, ALLE PROCEDURE DI IMPLEMENTAZIONE E AD ALTRI ELEMENTI SPECIFICI DELL'AMBIENTE E SISTEMA INFORMATIVO.

In linea generale le regole dovrebbero indirizzare:

- identificazione e autenticazione degli utenti;
- UserId (naming convention, assegnazione etc..);
- Password (regole di assegnazione,lunghezza, sintassi, scadenza, etc.) o altri strumenti di autenticazione (es. smart cards);
- definizione e protezione delle risorse;
- protezione e personalizzazione del software di base;
- classificazione, protezione e accessi alle risorse utente;

- crittografia (algoritmi, distribuzione, etc..);
- registrazione, conservazione e consultazione dei log;
- individuazione di tentativi di intrusione;
- autorità di System e Security Administration.

Per seguire le regole di applicazione delle politiche della sicurezza è necessario definire Processi specifici che descrivano gli specifici passi operativi che le persone devono seguire.

Ad esempio alcuni dei principali processi gestionali, riguardano:

1. definizione e cancellazione di UserId;
2. assegnazione di privilegi;
3. assegnazione delle password;
4. autorizzazioni di accesso ai dati/transazioni;
5. gestione chiavi di crittografia;
6. richiesta/gestione/rinnovo certificati digitali;
7. analisi e gestione dei log.

3.10 GESTIONE DEL RISCHIO

Dopo aver individuato i rischi (analisi del rischio) e le politiche aziendali È necessario individuare gli obiettivi della sicurezza informatica.

È quello che viene fatto nella fase di gestione del rischio nella quale si stabilisce:

- Rischio da abbattere.
- Rischio residuo ritenuto accettabile.

PER GESTIRE CORRETTAMENTE IL RISCHIO INFORMATICO E' BENE:

1. Trasferire del Rischio dalla P.A. a soggetti che si assumano la sua responsabilità: sottoscrivere polizze assicurative che coprano alcuni rischi, generalmente legati alla distruzione fisica di sistemi;
2. Abbattere del Rischio: adottare un insieme di contromisure di natura fisica, logica ed organizzativa, che possano fornire protezione in diverse maniere:
    - ridurre la minaccia;
    - ridurre la vulnerabilità;
    - ridurre l'impatto di eventi accidentali;
    - rilevare un evento accidentale;
    - aiutare nel recovery di un evento accidentale.

La decisione se implementare o meno un contromisura è una decisione strategica e viene influenzata da numerosi fattori differenti di carattere economico, organizzativo ecc.

MA

E' NECESSARIO DOPO QUESTA FASE AVERE DETERMINATO TUTTE LE CONTROMISURE POTENZIALMENTE NECESSARIE.

L'individuazione della specifica strategia di abbattimento del rischio e quindi le contromisure da adottare.

COSTITUISCE L'INPUT PER CONSENTIRE LO SVILUPPO DEL PIANO OPERATIVO DI IMPLEMENTAZIONE DELLE CONTROMISURE.

3.11 IL PIANO OPERATIVO

Una volta definite le risorse da proteggere, le strategie di contenimento del rischio ed il livello ritenuto accettabile, si procede con la:

STESURA DEL PIANO OPERATIVO

Che consente di determinare le contromisure più idonee

LA CUI ESECUZIONE È REGOLATA DALLE PRIORITA' ESPRESSE DALL'AMMINISTRAZIONE E DAI TEMPI RELATIVI ALL'EVOLUZIONE COMPLESSIVA DEL S.I.

DOPO AVER DEFINITO IL RISCHIO E LE CONTROMISURE DA ADOTTARE, CIOE' DOPO AVER DEFINITO LE RISORSE DA PROTEGGERE, LE STRATEGIE DI ABBATTIMENTO DEL RISCHIO ED IL LIVELLO DI RISCHIO RITENUTO ACCETTABILE

SI PROCEDE CON LA STESURA DEL PIANO OPERATIVO

Questo passo consente di determinare, tra l'insieme delle contromisure (funzioni di sicurezza) di natura fisica, logica ed organizzativa individuate:

- quali siano le più idonee
- verificarne la fattibilità,
- stabilirne le priorità di attuazione valorizzandone le mutue interdipendenze, per una copertura dei rischi sulla base degli obiettivi posti dalle Politiche.

Il piano operativo contiene:

1. l'individuazione dell'insieme delle attività di sviluppo della sicurezza;
2. il Piano Generale di attuazione;
3. le sinergie tra i diversi interventi;
4. le possibili alternative di realizzazione;
5. l'indicazione di tempi, risorse (materiali ed economiche) e competenze.

Per sviluppare il piano è necessario considerare:

1. Sicurezza Fisica;
2. Sicurezza Logica;
3. Sicurezza Organizzativa;
4. Piano di Continuità Operativa.

3.12 SICUREZZA FISICA E SICUREZZA LOGICA

La sicurezza può essere di due tipi:

1. fisica;
2. logica:

- la sicurezza fisica protegge le persone che operano sui sistemi, le aree e le componenti del sistema operativo
- la sicurezza logica protegge le informazioni e, di conseguenza, i dati, le applicazioni, i sistemi e le reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro destinazione e manutenzione nel tempo.

Sicurezza Fisica

LA SICUREZZA FISICA PROTEGGE LE PERSONE CHE OPERANO SUI SISTEMI, LE AREE E LE COMPONENTI DEL SISTEMA INFORMATIVO.

I requisiti di sicurezza fisica variano considerevolmente in funzione delle dimensioni e dell'organizzazione del Sistema Informativo le relative contromisure sono:

- **Sicurezza di area**: la sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle computer room rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.
- **Sicurezza delle apparecchiature hardware**: la sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in quest'area, come anche la protezione da manomissione o furti.

Sicurezza Logica

LA SICUREZZA LOGICA RIGUARDA LA PROTEZIONE DELL'INFORMAZIONE E, DI CONSEGUENZA, DI DATI, APPLICAZIONI, SISTEMI E RETI, SIA IN RELAZIONE AL LORO CORRETTO FUNZIONAMENTO ED UTILIZZO, SIA IN RELAZIONE ALLA LORO GESTIONE E MANUTENZIONE NEL TEMPO.

Le contromisure ad essa correlate sono l'insieme di misure di sicurezza di carattere tecnologico (Information and Communication Technology) e di natura procedurale ed organizzativa, le quali intervengono nella realizzazione del livello di sicurezza da raggiungere.

A causa dell'eterogeneità dei sistemi, delle reti e delle applicazioni che caratterizzano l'architettura dei Sistemi Informativi della PA, la realizzazione della Sicurezza Logica deve essere pensata in termini architetturali, in funzione della realizzazione di uno specifico Sistema di Sicurezza Logica.

Tale architettura di sicurezza si basa sull'individuazione di Servizi di Sicurezza cioè le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme, a tutti i livelli di elaborazione.

1. Autenticazione;
2. Controllo Accessi;
3. Confidenzialità;
4. Integrità;

5. Non Ripudio.

I Meccanismi di Sicurezza: rappresentano le modalità tecniche attraverso cui è possibile realizzare i servizi di sicurezza:

1. Cifratura;
2. Firma Digitale;
3. Meccanismi per il controllo degli accessi;
4. Integrità dei dati;
5. Meccanismi per l'autenticazione;
6. Traffic Padding ovvero saturazione del traffico in rete;
7. Controllo Instradamento;
8. Notarizzazione.

La definizione dell'architettura di sicurezza logica deve rispondere alle seguenti domande:

1. Quali funzioni di sicurezza devono essere garantite e per quali beni?
2. Con quali meccanismi di sicurezza è conveniente realizzare tali funzioni?
3. In quali livelli dell'architettura del sistema informatico devono essere collocati i diversi meccanismi?

INOLTRE PER: INDIVIDUARE LE FUNZIONI DI SICUREZZA DA GARANTIRE È necessario considerare i risultati della precedente attività di analisi dei rischi, delle politiche di sicurezza e della gestione del rischio.

INDIVIDUARE I MECCANISMI DI SICUREZZA DA UTILIZZARE E LA LORO COLLOCAZIONE AI DIVERSI LIVELLI DELL'ARCHITETTURA DEL SISTEMA INFORMATICO è necessario procedere ad una specifica attività di progettazione. Tale attività richiede notevole esperienza tecnica e progettuale ed è opportuno sia condotta da personale esperto e qualificato. Sostanzialmente si tratta di effettuare:

1. Analisi dei meccanismi attualmente in uso, verifica della loro congruenza con gli obiettivi di sicurezza, valutazione della loro efficacia ed efficienza.
2. Valutazione dell'allocazione di tali meccanismi all'interno dell'architettura in relazione ai beni da proteggere.
3. Analisi e verifica dell'utilizzo degli attuali meccanismi di sicurezza e della loro manutenzione.
4. Valutazione dell'introduzione di nuovi meccanismi in funzione di:

- nuovi beni da proteggere;
- nuovi servizi di sicurezza da realizzare;
- integrabilità dei nuovi meccanismi con quelli attualmente in uso;
- garanzia del mantenimento del livello di sicurezza;
- efficacia ed efficienza dell'architettura di sicurezza nel suo complesso;
- scalabilità, gestibilità e controllo dell'architettura di sicurezza nel suo complesso;
- alternative in relazione alle diverse architetture elaborative presenti nel S.I.A.;
- procedure di implementazione, gestione e controllo;
- accettabilità della soluzione da parte dell'utente;

- formazione per i gestori e gli utenti;
- tempi di implementazione;
- costi di implementazione e di gestione.

3.13 CONTROLLO DEGLI ACCESSI ANTIVIRUS

I computer possono essere colpiti da virus cioè da programmi scritti per generare intenzionalmente qualche forma di danneggiamento a un computer o ad una rete. **E' necessario aver installato un antivirus suk proprio PC e mantenerlo aggiornato.**

Un virus informatico può dar luogo a:

- danni all'hardware
- danni al software;
- danneggiamento di dati (integrità)
- perdita di tempo impiegato a ripristinare le funzioni del sistema;
- infezioni di altri sistemi.

PER LIMITARE IL RISCHIO È NECESSARIO CONTROLLARE GLI ACCESSI O RIMUOVERE IL VIRUS DAL SISTEMA MEDIANTE APPOSITI PROGRAMMI.

TALE CONTROLLO DEVE GARANTIRE CHE TUTTI GLI ACCESSI AGLI OGGETTI DEL SISTEMA INFORMATIVO AVVENGANO ESCLUSIVAMENTE SECONDO MODALITÀ PRESTABILITE.

Per farlo è necessario definire:

1. Un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, aggiornamento, etc…) secondo le quali i vari soggetti possono accedere agli oggetti.
2. Un insieme di procedure di controllo (meccanismi di sicurezza) che controllano se la richiesta di accesso è consentita o negata, in base alle suddette regole (validazione della richiesta).

Per garantire quanto sopra esposto, è indispensabile prevedere un meccanismo che costringa ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ad un calcolatore; il meccanismo sinora più usato a tale scopo è quello delle password.

Si concede cioè all'utente una coppia "User-Id e password", al livello del sistema operativo e/o per ogni applicazione (di solito in numero limitato), al cui accesso quell'utente è abilitato.

IL MECCANISMO DELLE PASSWORD, NON È PERÒ SUFFICIENTEMENTE ADEGUATO A GARANTIRE IL LIVELLO DI SICUREZZA RICHIESTO NELLA FASE DI AUTENTICAZIONE.

I problemi principali legati all'uso delle password sono: la scelta di password estremamente facili da indovinare da parte degli utenti e la possibilità di intercettarle quando transitano in rete.

Per far fronte a questi problemi è possibile individuare meccanismi di autenticazione forte che consentono di rendere molto più sicura una qualunque fase di autenticazione. Tali meccanismi sono basati sul riconoscimento di un attributo posseduto dall'utente, come ad esempio Una caratteristica fisica, quale l'impronta digitale, la forma della mano, l'iride, la retina, o una caratteristica

comportamentale quale la firma, la voce; in questo caso parliamo di dispositivi di autenticazione biometrici.

Una password generata dinamicamente da un apposito dispositivo personalizzato per ciascun utente, in questo caso parliamo di one-time password.

I certificati digitali sono il frutto dei risultati della più recente branca della crittografia, la crittografia a chiave asimmetrica. Al fine di utilizzare tali meccanismi è necessario fare riferimento ad una PKI (Public Key Infrastructure), cioè una infrastruttura che emette certificati digitali e che provvede alla loro gestione: pubblicazione in rete, revoca, sospensione e aggiornamento.

Oltre alla fase di identificazione ed autenticazione dell'utente, indipendentemente dal meccanismo di autenticazione utilizzato, si deve provvedere al controllo dell'accesso agli oggetti del sistema informativo. I sistemi operativi sono spesso dotati di meccanismi di sicurezza interni, i quali controllano se la richiesta di accesso sia consentita o negata. Come è già avvenuto per i mainframe, l'utilizzo di appositi strumenti di controllo accesso esterni, amministrabili in modo semplice e sicuro, agevolano il compito del gestore della sicurezza logica. Tali strumenti, oltre ad agevolare l'amministrazione della sicurezza attraverso semplici definizioni di regole di accesso agli oggetti (es.: file, directory, comandi), sono anche in grado di offrire un livello di sicurezza maggiore.

Antivirus

I computer virus sono i rappresentanti più noti di una categoria di programmi scritti per generare intenzionalmente una qualche forma di danneggiamento a un computer o ad una rete, indicati con il termine generico di codice maligno. Considerato che, un virus informatico può dar luogo a:

1. danni all'hardware;
2. danni al software;
3. danneggiamento di dati (integrità);
4. perdita di tempo impiegato a ripristinare le funzioni del sistema;
5. infezione di altri sistemi;

diviene necessario che le Amministrazioni attribuiscano la debita priorità all'adozione di iniziative di difesa, avviando una protezione sistematica dei propri sistemi informatici e dei dati in essi custoditi e gestiti, contro la minaccia rappresentata da virus, macro virus e worm.

Tali programmi sono in grado, senza alcun intervento dell'utente, di :

1. infettare altri programmi, cioè creare copie di sé stessi su altri programmi presenti nel sistema;
2. insediarsi nella tabella di partizione e nel settore di boot del disco rigido, dove attende il verificarsi di un determinato evento, per poter assumere il controllo di alcune funzioni del sistema operativo, con il fine di svolgere azioni dannose per cui è stato programmato:
3. inserire operazioni automatizzate (c.d. macroistruzioni) in documenti di testo, di archivio o di calcolo, dagli effetti indesiderati e nocivi;
4. autoreplicarsi all'interno del sistema, al fine di saturarlo.

Le azioni di danneggiamento possono andare dalla modifica del contenuto di alcuni file residenti sull'hard disk, alla completa cancellazione dello stesso; dall'alterazione del contenuto del video, all'impostazione hardware della tastiera. Definire una architettura antivirus, composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico, è la migliore difesa contro i virus informatici.

3.14 CONTROLLO DEL SOFTWARE

I principali punti di debolezza di un sistema informatico sono il sistema operativo e le sue applicazioni cioè i programmi che in esso girano.

Può succedere che attraverso lo sfruttamento di errori (bug) presenti in questi programmi, un estraneo riesca a guadagnare un accesso al sistema

In questo caso è ovviamente necessario adottare contromisure idonee che possono essere di due tipi:

- L'aggiornamento costante dei prodotti,
- La verifica periodica dell'installazione e della configurazione dei prodotti software.

IL SISTEMA OPERATIVO E LE APPLICAZIONI SONO TRA I PRINCIPALI PUNTI DI DEBOLEZZA DI UN SISTEMA INFORMATICO.

Può succedere che, attraverso lo sfruttamento di errori (bug) presenti in questi programmi, un estraneo riesca a guadagnare un accesso al sistema.

Le contromisure da adottare in questo caso possono essere di due tipi:

1. L'aggiornamento costante dei prodotti, che avviene non appena è scoperto un bug che compromette la sicurezza del sistema; tale procedura è nota come installazione di patch.
2. La verifica periodica dell'installazione e della configurazione dei prodotti software; un errore, anche minimo in questa fase, può trasformare un prodotto che dovrebbe contribuire a migliorare la sicurezza di un sistema (come ad esempio un firewall) nel prodotto che compromette ogni misura.

Numerose mailing list, gruppi di discussione e siti sono già attivi da tempo sull'argomento, quindi, sarebbe opportuno che gli amministratori di rete monitorassero costantemente queste fonti di informazioni ed aggiornassero i sistemi operativi. Ogni aggiornamento del software dovrebbe essere registrato in una specifica base dati.

3.15 RISERVATEZZA E AUTENTICITA' DEI DATI

Un sistema informativo sicuro deve rispondere ad alcuni requisiti

- **disponibilità**: l'informazione ed i servizi che eroga, devono essere a disposizione degli utenti del sistema, compatibilmente con i livelli di esercizio;
- **integrità**: l'informazione e di servizi erogati possono essere creati, modificati o cancellati, solo dalle persone autorizzate a svolgere tale operazione;
- **autenticità**: garanzia e certificazione della provenienza dei dati;

- **confidenzialità** o riservatezza: l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

La riservatezza rete ha l'obiettivo di contrastare i cosiddetti attacchi passivi, ovvero quelli tesi a carpire in modo non autorizzato il contenuto di informazioni o l'ubicazione degli interlocutori o la struttura del sistema telematico.

A seconda dei requisiti di sicurezza definiti dalle politiche, i servizi della riservatezza potranno essere:

- **Riservatezza dei dati**: protezione di tutti i dati trasmessi e ricevuti.
- **Riservatezza della Connessione**: protegge solo i dati di una particolare connessione selezionandoli in funzione degli indirizzi di rete o altro.
- **Riservatezza dei campi selezionati**: per garantire la riservatezza di particolari informazioni che risiedono in specifici campi.
- **Riservatezza del flusso di traffico**: per proteggere informazioni sulla quantità o la direzione del traffico dati.

Il meccanismo attualmente più diffuso per garantire la confidenzialità del traffico di rete è costituito dalla VPN (Virtual Private Network). Si tratta di un meccanismo che consente la cifratura del traffico tra due punti di una rete, in modo trasparente rispetto all'utente stesso. Requisito fondamentale per realizzare una VPN è che le due entità coinvolte siano tra loro compatibili nello svolgimento della suddetta funzione. Una volta predisposta una VPN tra due punti della rete, tutti i pacchetti di informazione tra questi punti sono cifrati/decifrati dai due dispositivi in questione, automaticamente e senza nessun intervento dell'utente, il quale viene tuttavia garantito sulla riservatezza delle informazioni trasmesse.

Strumenti per la Riservatezza ed Autenticità dei Dati

I dati conservati in un sistema informatico, devono essere protetti da letture e/o modifiche da parte di utenti non autorizzati. Due sono i momenti principali in cui tali dati devono essere difesi: l'accesso in locale e la trasmissione in rete.

Nel caso in cui i dati da proteggere risiedano su basi di dati è necessario ricorrere a prodotti che implementino politiche di autorizzazione per l'accesso ai dati, possibilmente legati a meccanismi di autenticazione forte degli utenti.

Per la protezione di dati conservati su file si possono utilizzare strumenti genericamente chiamati crypto file system. Tali strumenti utilizzano tecniche crittografiche e consentono di cifrare il contenuto dei file, in modo tale che lo stesso contenuto possa essere letto solo da utenti in possesso di un particolare codice, garantendo così la riservatezza dei dati.

3.16 AUTENTICAZIONE

Per essere affidabile un sistema deve anche poter assicurare che il ricevente sia garantito sull'autenticità del mittente e dei dati ricevuti. Ciò può essere realizzato in due modi:

- autenticazione per entità di pari livello

- autenticazione della sorgente dei dati

Il servizio garantisce l'entità ricevente sull'autenticità dell'entità mittente e dei dati ricevuti e può essere implementato in due modalità:

Autenticazione per entità di pari livello: garantisce la mutua autenticazione tra entità di pari livello interconnesse durante la fase iniziale del colloquio, e nel corso del trasferimento dei dati.

Autenticazione della sorgente dei dati: garantisce al ricevente l'autenticità dell'identità del mittente per ogni pacchetto inviato in trasmissione.

3.17 SICUREZZA ORGANIZZATIVA

PER RAGGIUNGERE UN LIVELLO DI SICUREZZA ADEGUATO ALLE POLITICHE AZIENDALI LE MISURE TECNOLOGICHE sono necessarie ma…

NON SONO SUFFICIENTI

È NECESSARIO ADOTTARE UNA SERIE DI NORME E PROCEDURE CHE SERVONO A REGOLAMENTARE GLI ASPETTI ORGANIZZATIVI E LE FASI DI LAVORO.

Ad esempio, prima di scaricare un documento dalla rete è importante avviare sempre un antivirus, ogni documento che viene ricevuto va inviato in posta elettronica all'ufficio protocollo.

L'insieme di queste procedure regolamentano:

documenti, utilizzo del software, password, i virus, la posta elettronica, le risorse informatiche, i supporti rimovibili, magnetici e ottici, la rete, la sicurezza dei personal computer portatili, i comportamenti illegali, le norme disciplinari, i riferimenti normativi.

Il Processo della Sicurezza dei Sistemi Informativi Automatizzati richiede che, accanto all'adozione di misure tecnologiche precedentemente illustrate…

SIANO DEFINITE UNA SERIE DI NORME E PROCEDURE MIRANTI A REGOLAMENTARE GLI ASPETTI ORGANIZZATIVI DEL PROCESSO MEDESIMO.

Gli aspetti organizzativi della Sicurezza dei Sistemi Informativi Automatizzati riguardano principalmente:

1. La definizione di ruoli, compiti e responsabilità, per la gestione di tutte le fasi del processo Sicurezza.
2. L'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate

Ogni Amministrazione, in relazione alla propria particolare struttura organizzativa e ruoli del personale, definirà specifici compiti e responsabilità. Le principali procedure organizzative emanate ed adottate per la Sicurezza dei Sistemi Informativi Automatizzati sono:

1. Procedure di Gestione delle Contromisure di Sicurezza Logica;
2. Procedure di Gestione specifiche per la Sicurezza della Rete;
3. Procedure di Controllo dei Sistemi di Sicurezza;
4. Procedure di Controllo del Ciclo di Vita del Software;
5. Procedure di Controllo per la Gestione delle Operazioni;
6. Procedure per la Gestione degli Incidenti;

7. Procedure per la Continuità Operativa;
8. Procedure per il Personale.

Queste procedure regolamentano:

1. **Documenti**: accesso ai documenti, Conservazione dei documenti, Consegna documenti, Distruzione;
2. **Utilizzo del software**: installazione, licenze d'uso, modalità d'uso;
3. **Password**: modalità di assegnazione, gestione ed utilizzo, validità nel tempo;
4. **I virus informatici**: misure preventive, regole operative, norme sull'utilizzo dei programmi antivirus;
5. **La posta elettronica**: norme generali, utilizzo corretto, attivazione del servizio;
6. **Le risorse informatiche**: generalità, Diritto d'Uso, Autorizzazioni, Dismissione, Installazione delle postazioni, Ergonomia e salute del lavoratore, Sicurezza ambientale, Protezione da furti, Blocco fisico dell'apparato, Blocco dell'avvio da disco floppy, Protezioni logiche della risorsa;
7. **I Supporti rimovibili, magnetici e ottici**: Supporto di memorizzazione fisso o rimovibile, Distruzione dei supporti magnetici e ottici;
8. **La rete**: Gli utenti di rete, Directory condivise, Monitoraggio e Gestione, Backup Centralizzato di rete, Utilizzo della rete;
9. **Sicurezza dei Personal Computer portatili;**
10. **Comportamenti illegali;**
11. **Norme disciplinari;**
12. **Riferimenti Normativi.**

Un ulteriore aspetto inerente la Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sull'affidabilità degli apparati. È necessario prendere tutte le precauzioni affinché i computer e tutti gli apparati utilizzati per l'erogazione dei servizi, non siano un punto di criticità del sistema.

Al di là di tutti quelli che sono i controlli già presenti sul materiale che va acquistato, è importante creare una banca dati di tutte le dotazioni HW, SW e di trasmissione dati della P.A.. È importante che questo comune archivio sia tenuto aggiornato con le sostituzioni, riparazioni e con i consumi delle apparecchiature. La banca dati dei sistemi informativi, se correttamente gestita, darebbe una visione storica e precisa del patrimonio, arricchita d'informazioni estremamente utili e statistiche sul grado di affidabilità e uso dei sistemi; sarebbe, di conseguenza, di grande aiuto nei processi di acquisto ed in quelli di pianificazione degli investimenti e delle scorte e materiali di consumo.

Nell'acquisto delle apparecchiature bisognerebbe prevedere sistemi di protezione elettrica della stesse, quali stabilizzatori di corrente e apparecchiature UPS.

Per HW utilizzato in attività di fondamentale importanza, come per il conseguimento degli obiettivi istituzionali, è importante prevedere l'impiego di apparati che più e meglio di altri garantiscano ridondanza ed affidabilità (Fault Tolerance).Oltre a regolamentare il comportamento dei propri utenti, è

necessario anche regolamentare quello di utenti esterni (ad esempio consulenti e fornitori) che operano con il Sistema Informativo Automatizzato, o comunque che sono abilitati a connettersi con esso.

Approfondimento:

La Sicurezza Informatica può essere definita come l'insieme delle misure di carattere procedurale - organizzativo e tecnologico atte a garantire, la Riservatezza, l'Integrità e la Disponibilità delle informazioni e dei servizi, gestiti o erogati.

Nel documento sarà utilizzato l'acronimo RID proprio per definire questi tre ambiti per ognuno dei quali sarà necessario attuare una serie di procedure e misure specifiche.

Il documento prenderà quindi in esame la necessità di costituire un Sistema di Gestione della Sicurezza Informatica che può essere applicato tanto alle Aziende quanto alla PA nelle sue molteplici e diverse articolazioni.

I fattori contribuenti alla necessità di un SGSI sono:

- la necessità di protezione dei beni (asset)
- le debolezze della tecnologia (intrinseche e non)
- Gli elementi costitutivi della natura di SGSI sono:
- l'Area tecnologica
- l'Area organizzativa
- l'Area legale

Va da sé che maggiore è il valore che si assegna al bene da proteggere (asset) maggiore dovrà essere lo sforzo, anche finanziario, che dovrà essere compiuto per la protezione del bene medesimo.

I Sistemi di Gestione per l'Information Security (detti anche Information Security Management Systems, o "ISMS") hanno come obiettivo principale l'implementazione di adeguati controlli, sotto forma di strutture organizzative, policy operative, istruzioni, procedure e funzioni software, atti ad assicurare il soddisfacimento di specifici obiettivi di sicurezza stabiliti dall'azienda

«In Italia il problema della vulnerabilità dei sistemi di controllo è preso seriamente dalle Autorità.

Alcune infrastrutture di controllo e gestione distribuite sul territorio nazionale sono giudicate critiche e "degne" di un livello di protezione superiore alla media perché un loro blocco porterebbe gravi danni a tutto il sistema-Paese….»(Computerwold–IDG –Maggio 2005).

Sovente si tende ad identificare il termine riferito alla *sicurezza informatica* con le norme relative alla Privacy di cui al D.L.vo 193/2006 che rappresentano invece uno specifico aspetto della più complessa problematica.

Oggi, rispetto al passato, con la crescita dell'uso di nuove tecnologie come i dispositivi portatili, la virtualizzazione dei sistemi operativi, la banda larga e le connessioni flat, le reti Wireless (Wi-Fi, Wi-Max e Bluetooth), nonché con l'introduzione sempre più diffusa delle tecnologie RFID e VoIP e dei software per il file sharing e quanto altro ancora 'vive' nel panorama delle ICT la battaglia per la protezione dei dati assume un rilievo tale che non ci si può più affidare a soluzioni 'fai da te'.

La sicurezza delle informazioni è quindi un insieme di misure ad ampio respiro finalizzato da una parte a proteggere le informazioni elettroniche per mezzo della sicurezza informatica e dall'altra a proteggere le informazioni cartacee attraverso misure organizzative.

A livello europeo lo standard BS 7799:1 (British Standard Institute) prende in considerazione l'intero processo di gestione delle informazioni e prevede il coinvolgimento e l'integrazione di tutti gli elementi della catena del valore dell'impresa, ovvero le persone, i processi, le tecnologie, al fine di consentire una corretta gestione delle informazioni e ridurre il rischio di danneggiamenti, furti, accessi non autorizzati. La BS 7799:1 è recepita nella normativa ISO 17799 del 1995 .

Alla BS 7799:1 si affianca la BS 7799:2 che recentemente è stato pubblicata come **ISO 27001** ed è certificabile, mentre l'ISO 17799 viene definito come manuale pratico (Security Code of Practice) privo di valore normativo, ovvero una delle tante metodologie adottabili per soddisfare i requisiti della norma ISO 27001.

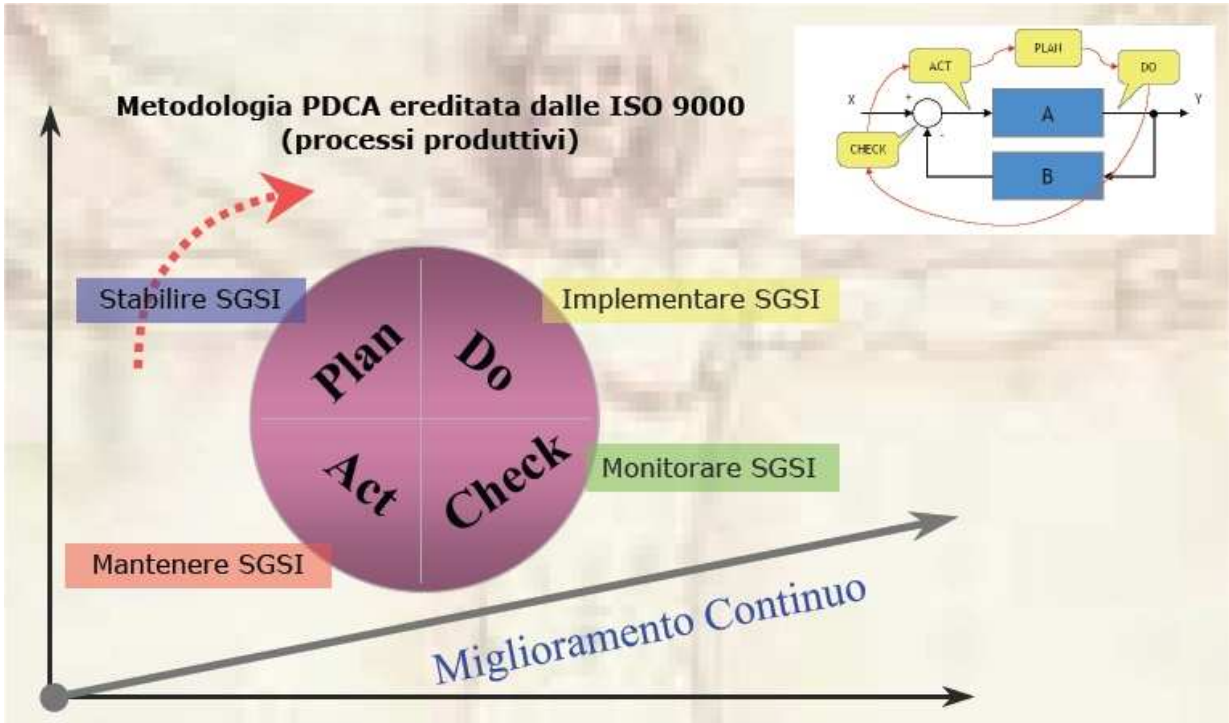
Tale norma introduce il concetto di "Sistema di Gestione", uno strumento che permette di tenere sotto controllo in modo sistematico e continuativo tutti i processi legati alla sicurezza delle informazioni tramite la definizione di ruoli, responsabilità e procedure formali sia per l'operatività aziendale, che per la gestione delle emergenze.

In Italia, per la Pubblica Amministrazione, il 16 Gennaio 2003, il Ministero per l'Innovazione Tecnologica, d'intesa con il Ministero delle Comunicazioni hanno rilasciato la c.d. "Direttiva Stanca per la PA" in cui sono descritte le Best Practice. Tali procedure fanno esplicito riferimento alla norma BS in questione.

Gli Standard sono un presupposto di valore in quanto:

- Definiscono degli importanti elementi di garanzia anche contrattuali, interpretabili come "livelli di servizio", oppure come specifiche organizzative condivise tra le parti.
- Definiscono la macro-struttura organizzativa per l'implementazione, il controllo e per il miglioramento continuo per definiti aspetti del sistema di gestione.
- Introducono l'Auditing interno, quale processo per il monitoraggio della presenza e dell'efficacia dei controlli, nonché in considerazione della necessità della pianificazione delle attività di miglioramento
- Definiscono le condizioni per una corretta gestione dei diversi rischi, compresi quelli di natura ambientale, tra i quali quelli relativi alla sicurezza delle informazioni.

Ciascun Ente - Azienda - Organizzazione, dovrebbe disporre di un "**Sistema di Gestione della Sicurezza delle Informazioni**", ed osservare il modello processuale definito dal BS che propone la metodologia - di derivazione del processo di controllo di qualità ancorché applicata in maniera più stringente e severa – Plan, Do, Check, Act. (Pianificare, Eseguire, Verificare, Mantenere) per un'analisi dei rischi e la successiva predisposizione del documento programmatico della sicurezza e del documento per la gestione degli incidenti.



La rappresentazione schematica in quattro settori circolari ideata da Edwards Deming, che nel 1946 introdusse in Giappone il controllo di qualità.

Modello processuale proposto:

FASE 1: PLAN – Pianificazione e scelta del SGSI
FASE 2: DO – Implementazione del SGSI
FASE 3: CHECK – Monitoraggio e revisione del SGSI
FASE 4: ACT – Mantenimento e miglioramento del SGSI

La fase di **Plan** consiste nell'identificare il problema, nell'analizzarlo, nell'individuare le cause reali, nel definire e pianificare le azioni correttive.

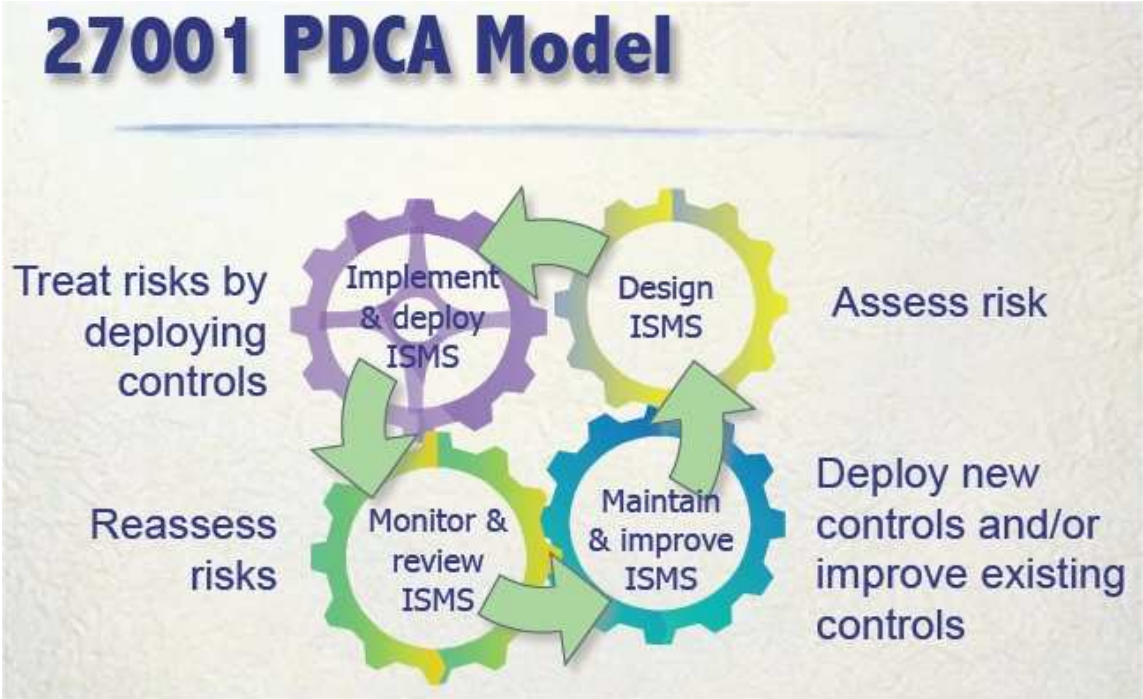
Obiettivi della pianificazione sono:

- Razionalizzare gli interventi
- Condividere gli obiettivi
- Condividere i processi
- Mantenere traccia del processo decisionale
- Disporre di uno strumento per verificare il raggiungimento degli obiettivi
- Predisporre i piani finanziari

La fase di **Do** consiste nel preparare e applicare le azioni pianificate, a livello di test.

La fase di **Check** consiste nel verificare i risultati delle azioni intraprese, confrontandoli con gli obiettivi attesi.

La fase di **Act** consiste nello standardizzare e consolidare se il check è stato positivo, introducendo le modifiche nel ciclo produttivo, oppure nel preparare un nuovo ciclo PDCA se il check ha rilevato nuovi inconvenienti.



Le parole chiave

Riservatezza: è la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la visione da parte di soggetti terzi non autorizzate. La riservatezza risulta necessaria per la trasmissione dei dati sensibili ed è dunque uno dei requisiti che garantiscono il rispetto della vita privata degli utenti.

Le informazioni sono un bene (asset) che deve essere protetto da minacce specifiche, al fine di garantire la continuità del servizio e minimizzare le eventuali perdite di dati.

Rientra in questo ambito la problematica dell'autenticazione sicura ovvero dell'identificazione certa ed univoca del soggetto che accede al sistema ed ai dati.

- **Integrità**: è la veridicità - conferma che i dati trasmessi, ricevuti o conservati siano completi e non alterati. Il requisito dell'integrità dei dati è significativamente importante rispetto alle procedure di conclusione dei contratti o quando è indispensabile garantire l'accuratezza dei dati stessi come nel caso di dati medici, dati relativi alla progettazione industriale, ecc.
- **Disponibilità**: è l'esigenza che i dati siano sempre accessibili e che i servizi funzionino anche nel caso di interruzioni dovute, ad esempio, alla cessazione dell'energia elettrica, a eventi disastrosi naturali, eventi imprevisti e/o ad attacchi di pirateria informatica.

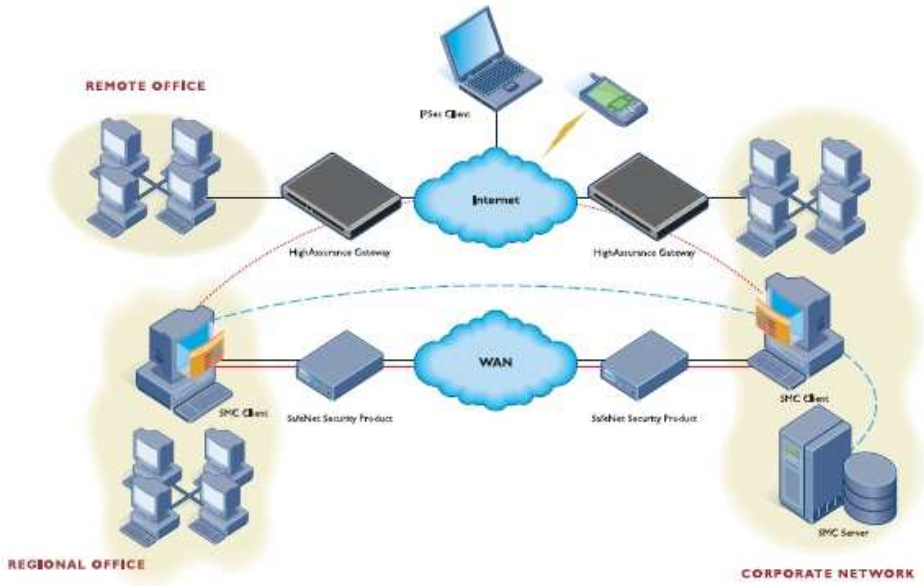
E' un requisito di primaria importanza nei casi in cui l'indisponibilità di una rete di comunicazione può generare disfunzioni rispetto all'erogazione del servizio.

Gli attacchi informatici

Preliminarmente è possibile affermare che la fonte principali di attacchi informatici è insita nella debolezza del protocollo di comunicazione TCP/IP.

Nel 1987 viene arrestato ad Hannover uno dei più famosi hackerdella storia: Matthias Speerche riesce a violare l'accesso di molte macchine e reti tra cui anche quelle di basi militari USA. E' catturato grazie alla collaborazione di un SM Cliff Stollcon FBI, CIA ed NSA mediante l'uso di un sito "Honeypot". (cfr Volume: The cockoo's egg).

Nel novembre del 1988 R. Morris sfrutta una vulnerabilità del O/S SunOS scrivendo un programma worm, composto da circa 150 righe di codice sorgente in linguaggio C. Tale programma si replica e si trasferisce automaticamente sulle macchine raggiunte in rete.



Un potenziale pericolo deriva inoltre non solo dall'eventuale accesso ai dati dall'esterno e sulla rete, ma dalla comprimissione del parco PC a causa di virus, worm, programmi di file-sharing installati dagli addetti, root-kit.

Inoltre a livello statistico il 35% degli attacchi alle reti informatiche proviene dall'interno, ovvero da personale appartenente all'Ente – Azienda e ciò dovrà essere considerato attentamente per assumere tutte le adeguate misure di protezione in merito.

Giornalmente viene combattuta una più o meno silenziosa battaglia nella rete tra coloro che tentano di violare sistemi informatici e coloro che provano ad impedire che ciò accada. Purtroppo non tutti coloro che hanno subito un attacco informatico denunciano il fatto alle Autorità più per paura di risultare compromessi di fronte ai loro clienti che altro.

Un utente malevolo che desideri reperire informazioni nella rete può utilizzare, sul proprio computer, alcuni applicativi progettati per interfacciarsi con i server ed inviare a questo ultimi comandi e/o codice al fine di divenirne

proprietario. Dunque l'oggetto principale degli attacchi informatici sono le informazioni.

Con il controllo dei sistemi informativi un attaccante può quindi compiere azioni dannose come rubare segreti industriali, alterare documenti e molto altro ancora come già detto.

I metodi di attacco

Le tipologie di attacco informatico possono essere molteplici. La maggior parte può essere categorizzata in determinate classi recepite ormai anche dalla letteratura in materia di sicurezza informatica.

Interruzione del servizio (DOS).

Gli attacchi di negazione del servizio (DoS, Denial of Service) sono attacchi rivolti a specifici host o reti. Questo tipo di attacco prevede solitamente l'invio a un host o router di una quantità di traffico superiore a quella che l'host o il router è in grado di gestire in un determinato intervallo di tempo, provocando così l'incapacità della rete di gestire il traffico e la conseguente interruzione del flusso del traffico autorizzato.

Gli attacchi di negazione del servizio possono avvenire in forma distribuita tra numerosi vettori di attacco ai danni di un obiettivo mirato. I computer oggetto dell'attacco vengono solitamente compromessi in qualche modo con l'installazione di un programma o uno script di software dannoso che consente agli autori dell'attacco di utilizzare tali computer per il flooding coordinato di traffico di rete verso altri computer o gruppi di computer. I computer violati vengono definiti zombi e questo tipo di attacco è detto attacco di negazione del servizio distribuita (DDoS, Distributed Denial of Service).

Intercettazione (sniffing).

I pacchetti possono essere intercettati durante il tragitto dal mittente al destinatario. Ciò è possibile utilizzando in rete i software denominati sniffer, oppure costringendo i pacchetti di informazione a variare il loro percorso in modo da portarli a transitare attraverso un calcolatore controllato dal malfattore. L'attacco è di tipo passivo (le informazioni vengono intercettate ma non modificate) e proprio per questo è piuttosto difficile da rilevare.

Esso è pericoloso per la riservatezza della comunicazione, se tra client e server vengono scambiate informazioni riservate. Infatti un attaccante sarebbe potenzialmente in grado di ricostruire i files trasmessi e quindi carpire eventuali dati riservati in essi contenuti.

L'autore di un attacco può tentare di catturare il traffico di rete con due finalità: per ottenere copie di file durante la loro trasmissione e/o per ottenere le password che gli consentirebbero di penetrare ulteriormente all'interno della rete. Gli hacker utilizzano sovente strumenti di sniffing dei pacchetti per registrare le connessioni TCP e ottenere copie delle informazioni trasmesse. Ad esempio il protocollo ARP (Address Resolution Protocol) può subire attacchi mediante altri strumenti appositamente predisposti, che reindirizzano il traffico IP attraverso il computer del pirata informatico, consentendogli di registrare tutte le connessioni.

Poiché alcuni protocolli, quali ad esempio il POP3 (Post Office Protocol 3) e l'FTP (File Transfer Protocol (FTP), inviano password non crittografate attraverso la rete, un pirata informatico che esegua lo sniffing della rete non avrebbe difficoltà a ottenere questo tipo di informazioni. Diverse applicazioni utilizzano un meccanismo challenge/response che evita il problema dell'invio di password in testo normale, ma migliora di poco la protezione. Il pirata informatico, pur non riuscendo a leggere direttamente la password, potrebbe comunque ottenere una copia del challenge/response mediante un attacco del dizionario.

La crittografia delle comunicazioni consente di proteggersi efficacemente contro lo sniffing della rete.

Modifica (Hijacking).

Questo tipo di attacco tenta di compromettere l'integrità delle informazioni trasmesse, ovvero rende possibile la modifica dei pacchetti nel tragitto dal mittente al destinatario. Di norma l'accesso e la manipolazione a distanza delle risorse critiche di una rete è permesso esclusivamente a personale autorizzato.

Un complicato sistema di identificazione impedisce l'accesso a chiunque non sia in possesso dei requisiti necessari.

Si pensi alle maggiori banche che si stanno attrezzando con sistemi multipli di identificazione, tra questi le *one shot password*.

Si tratta spesso di un token hardware che visualizza un codice one shot, valido per l'accesso via interfaccia web alla propria sessione sul server. L'autenticazione in rete diventa quindi molto più protetta: alle normali informazioni di login e password, l'utente deve aggiungere il codice aggiuntivo della *one shot password*, estremamente sicuro in quanto, oltre ad avere i vantaggi di portabilità di un token hardware, la password cambia ad ogni richiesta di accesso e vale solo per un tempo prefissato di un'unica sessione di lavoro.

In caso di riuscita di attacco tutti i pacchetti che partiranno dal client autorizzato potranno essere intercettati prima di arrivare al server. Questo permetterebbe all'ignoto malfattore di sostituirsi all'utente originario ereditandone tutti i privilegi e contemporaneamente aggirando i sistemi di sicurezza.

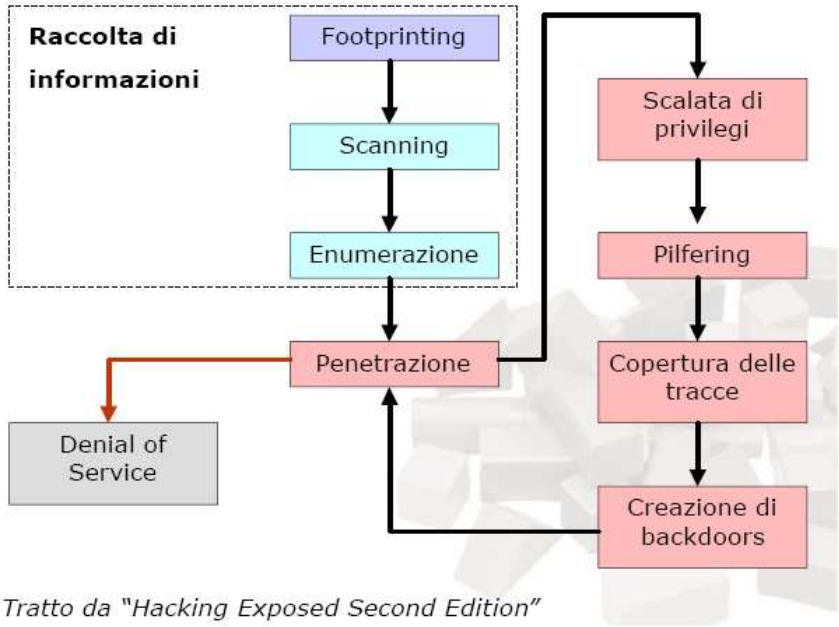
Spoofing - Sostituzione d'identità

I pericoli di **spoofing** di identità comprendono qualsiasi azione per ottenere o accedere illegalmente e utilizzare le informazioni di autenticazione di un'altra persona, ad esempio nome utente o password. Questa categoria di pericoli include gli attacchi di tipo "*man-in-the-middle*" e le comunicazioni di host affidabili con host non affidabili. Questo tipo di attacco è molto complesso e presenta numerose varianti. Il suo scopo è il tentativo di falsificazione di

identità. In pratica un attaccante può modificare, o creare ex novo, pacchetti di dati in modo che essi appaiano spediti da qualcun altro.

E' un attacco insidioso e può essere sfruttato sia per tentare di ottenere particolari privilegi sia per agire in modo anonimo nella rete.

Gli attacchi di tipo "*man-in-the-middle*" sono una tecnica comunemente impiegata dai pirati informatici consistente nel collocare un computer tra due computer che comunicano tra loro tramite una connessione di rete affinché il computer interposto rappresenti uno o entrambi i computer originali. Mediante questa tecnica, il pirata informatico dispone di un computer con una connessione attiva ai computer originali che gli consente di leggere e/o modificare i messaggi trasmessi da un computer all'altro, all'insaputa degli utenti dei due computer originali



Tratto da "Hacking Exposed Second Edition"

Un attacco può provocare dunque i seguenti eventi:

- Divulgazione/Sottrazione (**Disclosure**)
- Distruzione/Perdita (**Destruction**)
- Indisponibilità Momentanea (**Denial of Service, DoS**)
- Modifica (**Modification**)

Occorre pertanto studiare le tecniche di attacco in quanto:

- Ci permettono di evidenziare come sono sfruttate le diverse vulnerabilità e come più vulnerabilità interagiscono
- Possono essere utilizzate per l' implementazione della sicurezza attraverso opportune modifiche
- Nella implementazione della sicurezza un reale beneficio si ha imparando dagli errori: occuparsi delle vulnerabilità imparare dagli errori.

Nella gestione di un sistema per la sicurezza informatica (SGSI) fondamentale importanza assume **l'ethical hacking.** Per ethical hacking si

intendono tutte le attività di verifica coordinata e complessiva della sicurezza di un sistema, al fine di delineare il livello effettivo di rischio cui sono esposti gli asset e proporre eventuali azioni correttive per migliorare il grado di sicurezza.

Ethical perché vengono utilizzati gli strumenti e le tecniche tipiche degli attaccanti senza mettere a rischio integrità dei dati e continuità del servizio e viene inoltre garantita la riservatezza delle informazioni cui viene ottenuto accesso che, sovente, si rivelano particolarmente sensibili e preziose. Vengono poi fornite le indicazioni da seguire per migliorare lo stato di sicurezza, relativamente alle vulnerabilità individuate.

Phishing

In ambito informatico il phishing ("spillaggio (di dati sensibili)", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a messaggi che imitano grafico e logo dei siti istituzionali, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc. (Wikipedia)

Nella gestione di un sistema per la sicurezza informatica (SGSI) fondamentale importanza assume **l'ethical hacking.** Per ethical hacking si intendono tutte le attività di verifica coordinata e complessiva della sicurezza di un sistema, al fine di delineare il livello effettivo di rischio cui sono esposti gli asset e proporre eventuali azioni correttive per migliorare il grado di sicurezza.

Ethical perché vengono utilizzati gli strumenti e le tecniche tipiche degli attaccanti senza mettere a rischio integrità dei dati e continuità del servizio e viene inoltre garantita la riservatezza delle informazioni cui viene ottenuto accesso che, sovente, si rivelano particolarmente sensibili e preziose. Vengono poi fornite le indicazioni da seguire per migliorare lo stato di sicurezza, relativamente alle vulnerabilità individuate.

SGSI / ISMS (Sistema di Gestione della Sicurezza Informatica - Information Security Management System)

Un Sistema di Gestione della Sicurezza Informatica deve rispondere a molteplici esigenze quali:

- **Sicurezza delle reti** (Sicurezza perimetrale) e dei sistemi Firewall, Hardening O/S, Honeypot
- **Sicurezza del Contenuto** (Content Filtering) Antivirus, Sistemi di Intrusion Detection/Prevention (IPS/IDS), Log Correlation
- **Identity Management** (Gestione Identità Digitale) (Password, Single Sign On, Autenticazione sicura, Certificati Digitali, Biometria)
- **Autenticità e Segretezza delle Comunicazioni Crittografia**, VPN, Certificati Digitali, Firma Digitale
- **Business Continuity e Disaster Recovery** Business Continuity Planning, Backup, Restore (Conservazione e Ripristino Dati/Funzionalità)

- **Analisi Incidente e Forensic** (Documentazione probatoria) Trusted Computing, Conservazione dei Log.

Come è possibile gestire la sicurezza?

Implementare in sistema di gestione della sicurezza delle informazioni dunque significa:

- Delimitare l'ambito di applicazione del sistema ai processi rilevanti per il business;
- Definire una Policy interna della sicurezza;
- Analizzare e valutare i rischi;
- Gestire i rischi;
- Scegliere i controlli / misure da applicare;
- Redigere una dichiarazione di applicabilità e conformità legale

Nello specifico un SGSI deve prendere in esae, indagare e documentare:

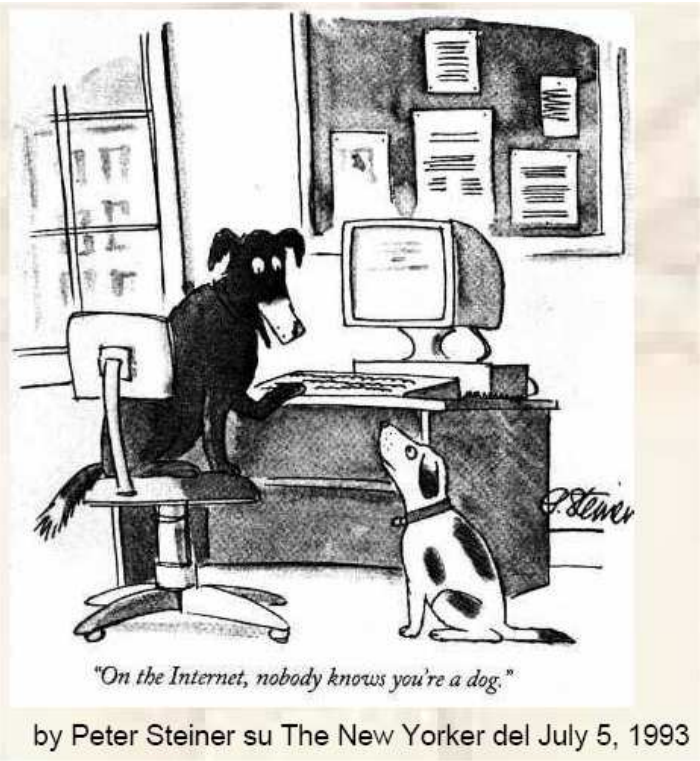
- la classificazione degli asset
- la sicurezza fisica
- la sicurezza di rete
- la sicurezza dei sistemi
- la gestione delle credenziali
- la gestione delle vulnerabilità
- la gestione degli incidenti e rischi
- il business continuity e disaster recovery
- il coordinamento e controllo dei processi
- le politiche utenti e amministrative
- la conoscenza, formazione e sensibilizzazione
- la conformità legale e normativa

Comportamenti degli utenti

Particolare attenzione quando si parla di sicurezza informatica va preliminarmente posta a concetti quali l'addestramento e la consapevolezza degli operatori che andranno istruiti e formati onde evitare pratiche che potrebbero, più o meno consapevolmente, mettere a rischio l'integrità del sistema informatico e quindi acnhe la riservatezza e la disponibilità dei dati.

In genere, le aziende e gli Enti di medie e grandi dimensioni si affidano ad esperti che installano e mantengono in piena efficienza una serie di applicazioni e dispositivi di sicurezza sulla rete interna. Nonostante questo attento lavoro di prevenzione, un fattore critico rimane al di fuori del controllo degli esperti: il fattore umano, vale a dire il comportamento degli utenti del sistema informatico, in particolare quando l'utente lavora da postazioni remote o utilizza lo stesso computer portatile a casa e in ufficio. Se poi si prendono in considerazione anche i dispositivi portatili che vengono quotidianamente collegati alla rete aziendale, come le chiavi USB, gli hard disk esterni o i PDA, è facile capire quanto il controllo possa diventare difficile. Senza la collaborazione dei singoli utenti, è praticamente impossibile garantire la protezione della rete aziendale. Ecco alcune regole di base per proteggere i dati.

Uso delle password



Password scritte sul classico post-it incollato al computer, inserite in un file o comunicate ad altre persone (non soltanto colleghi) rappresentano iniziative a rischio che continuano ad essere praticate nei luoghi di lavoro. È importante invece scegliere password difficile da indovinare ma facili da ricordare, non scriverla mai da nessuna parte, sostituirla sempre ad intervalli regolari e non comunicarla a nessuno.
I fattori di autenticazione dovrebbero rispettare tre principi :

- qualcosa che tu sai (PIN, password)
- qualcosa che tu hai (Smart Card, Token)
- qualcosa che tu sei (es. impronta digitale)

I sistemi possono adottare 3 metodi per la registrazione della password

- <u>Registrazione della password con testo in chiaro nel database delle password</u>

  Non esistono mascheramenti, cifratura e codifica. La password è di fatto contenuta in un database riservato. Se forzato, la sicurezza è nulla. E' frequente nelle applicazioni standard.
- <u>Cifrare la password prima di registrarla nel data-base delle password</u>

  La cifratura unisce un testo in chiaro ad una chiave segreta per creare una stringa complessa che può essere decifrata riutilizzando la stessa chiave. In altre parole: memorizzazione di password protetta da altra password. Chi possiede la seconda password può leggere il data-base in chiaro.
- <u>Utilizzo della tecnica di hashing</u>

  Un hash è il risultato di un algoritmo che modifica il testo in chiaro al fine di produrre una stringa complessa che rappresenti la password. Gli algoritmi di hashing sono formule a una via (non-invertibili) poiché è impossibile risalire alla password originale dato che non è possibile eseguire la formula in senso inverso. Per controllare la password

immessa, il sistema calcola ogni volta l'hash e lo confronta con l'hash contenuto nel data-base delle password

Le regole di complessità per la creazione di password

Per ottenere password complesse occorre utilizzare stringhe alfanumeriche contenenti caratteri appartenenti ad almeno 3dei 5 gruppi seguenti. Le password dovrebbero appartenere ad ognuno dei gruppi seguenti:

Gruppo	Esempio
Lettere minuscole	a, b, c, ….
Lettere maiuscole	A, B, C, ….
Numeri	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non alfanumerici	( ) ` ~ ! @ # $ % ^ & * - + = |
Caratteri Unicode	€, Γ, ƒ, e λ

Unicità delle password

La password è unica se è esclusiva di un particolare sistema e si distingue da tutte le altre password.

Per creare una password unica occorre seguire alcuni accorgimenti quali:

- Evitare di utilizzare password o frasi comuni oppure termini tratti dal dizionario
- Non utilizzare mai la stessa password più di una volta, soprattutto su sistemi diversi
- Evitare di affezionarsi troppo ad una password e continuare ad usarla anche ciclicamente
- Evitare parole o numeri legati alla propria persona, alla propria famiglia o all'ambiente di appartenenza
- Evitare pattern o sequenze prevedibili

Non conservare mai una password per più di un anno

Segretezza delle password

- Non condividere le password con altri.
- Evitare di registrare le password in modo non sicuro
- Non salvare le password nel browser web ed in altre applicazioni
- Eliminare password di posta elettronica contenenti password
- Cambiare sempre le password di default o assegnate automaticamente

Virus e malware

Il termine virus viene utilizzato nell'uso comune come sinonimo di malware e l'equivoco è alimentato dal fatto che gli antivirus permettono, talvolta, di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Di norma un malware è caratterizzato dall'intento doloso del suo creatore, non rientra dunque nella categoria dei bug che, essendo codice scritto male, non

è di fatto controllabile anche quando si sia osservata la massima diligenza nello sviluppo di un software.

I "Malware" sono dunque programmi o parti di programmi che hanno un effetto deleterio rispetto aulla sicurezza del computer. La parola vuole indicare vari termini come "Virus", "Worm" e "Trojan" ed anche altri meno noti quali "Rootkit", "Logicbomb" e "Spyware".

Per ognuna di queste categorie occorre porre in atto tutta una serie di contromisure al fine di ridurre il rischio.

I virus possono installarsi o essere presenti:

- nel settore di boot
- nei file eseguibili
- virus TSR (Terminate e Stay Resident)
- macro virus ovvero virus veicolati dalle macro degli applicativi software.

Cavalli di troia e spyware

I Cavalli di Troia sono stringhe di codice dannoso (software) mascherato come qualcosa di normale per far sì che vengano eseguite. Danneggiano il computer installando una backdoor o un rootkit o più sovente tentano di installare un dialer.

Gli Spyware sono software che si installano a insaputa dell'utente; sovente vengono scaricati anche inconsapevolmente da siti web che visitati.

Rootkits e backdoor

Sono software che creano meccanismi per accedere ad una macchina. Possono rimanere in ascolto su una porta o nascondere processi in memoria, modificando i file di log.

Nella gestione di un sistema informativo, più o meno complesso, fermo restando le vulnerabilità di sistema e le minacce fin qui esposte, è bene rimarcare che spesso l'anello debole è il fattore umano…..

Porre rimedio a questo vuol dire creare una cultura della sicurezza, investire quindi in formazione, educare al rispetto dei processi e delle procedure che anche se apparentemente noiose vanno osservate al fine di salvaguardare la riservatezza, l'integrità e la disponibilità dei dati.

I dispositivi di rete da 'sorvegliare'

Router.

Nella tecnologia delle reti informatiche un router, è letteralmente l'*instradatore*, è un dispositivo di rete che si occupa di instradare i pacchetti sulla rete. E' l'interfaccia tra la rete interna (LAN) ed Internet.

Switch

Nella tecnologia delle reti informatiche, uno switch è un dispositivo di rete che inoltra selettivamente i pacchetti ricevuti verso una ben

precisa porta di uscita. Uno switch possiede quindi l'intelligenza necessaria a riconoscere l'IP ovvero il PC di destinazione.

Hub

Nella tecnologia delle reti informatiche, uno Hub è un dispositivo di rete che inoltra i pacchetti ricevuti verso tutte le porte di uscita. A differenza dello *switch* NON possiede quindi l'intelligenza necessaria a riconoscere l'esatto IP ovvero il PC di destinazione.

Wireless

In informatica, il termine wireless (dall'inglese senza fili) indica i sistemi di comunicazione tra dispositivi elettronici, che non fanno uso di cavi. I sistemi tradizionali basati su connessioni cablate sono detti *wired*. Generalmente il wireless utilizza onde radio a bassa potenza.

Le reti wireless sono e ci si aspetta che saranno sempre più una importante forma di connessione per molte attività, soprattutto per le imprese. (Wikipedia) – Anche nelle scuole le reti *wireless* sono orami diffuse anche in considerazione del risparmio di spesa rispetto alla stesura di cavi nell'edificio.