

Infosecurity

“Servizi innovativi per le imprese.
La sicurezza in informatica”

“La sicurezza per lo sviluppo delle
reti e del mercato ICT”

Milano, 10 febbraio 2005

Pietro Varaldo
Direttore generale Federcomin

Apertura dei lavori

Il tema dell'**economia dei servizi innovativi**, scelto da **Infosecurity** per il Convegno di oggi, è un tema molto caro a Federcomin e non a caso il Presidente Tripi lo ha proposto in occasione della **Giornata dell'Innovazione** organizzata da Confindustria il 16 novembre a Parma.

I servizi innovativi rappresentano **una nuova economia che è ormai una realtà intorno a noi**: un'economia per realizzare appieno l'innovazione del Sistema-Paese.

Noi ci siamo impegnati nel tracciare quelle che possono essere considerate le **linee-guida** di un'economia dei servizi per l'innovazione del Paese:

- **favorire la competitività**
- porre il **cliente-cittadino** al centro dell'attività economica
- **utilizzare le tecnologie** per migliorare i livelli di efficienza e la qualità della vita

- **innovare l'impresa e la P.A.** (ieri è stato presentato il nuovo **Codice dell'amministrazione digitale**, con diritti e doveri del cittadino italiano della Società dell'Informazione)
- creare **nuove opportunità** per vincere la sfida dell'internazionalizzazione
- ripensare le **politiche di intervento pubblico**.

I **valori dell'impresa innovativa** risiedono, a nostro avviso, nei **prodotti e servizi** che l'impresa stessa produce, nella **qualità del servizio**, nel **confronto competitivo**, nel **mercato e nell'ambiente**.

Non a caso il tema della qualità è estremamente attuale, come conferma il recente **Rapporto elaborato da Cnipa e Federcomin** per la Pubblica Amministrazione.

Tuttavia, c'è ancora una **percezione diffusa di una insufficiente capacità innovativa**. E questo è il punto cruciale dell'arretratezza del nostro Sistema-Paese. Un ritardo che si spiega con la **difficoltà di superare la cultura manifatturiera**

che ha generato lo sviluppo industriale italiano, ma che da sola è inadeguata a cogliere i bisogni e le profonde trasformazioni introdotte dalle tecnologie dell'informazione e dalle sfide competitive legate alla globalizzazione.

In una nuova economia basata sulle **reti sempre più veloci** per assicurare più servizi a tutti e sulle applicazioni informatiche e della comunicazione, la **sicurezza è un aspetto determinante** per lo sviluppo di questo nuovo contesto tecnologico, oltre che di estrema attualità per la condivisione a livello globale dei grandi eventi del pianeta (dal terrorismo alle catastrofi naturali).

Oggi al concetto di sicurezza "fisica" si affianca, in misura crescente, quello di sicurezza delle infrastrutture immateriali e quello di sicurezza "allargata", coinvolgendo gli aspetti di fiducia – un esempio è il **Progetto Fiducia Federcomin** – o di protezione delle categorie deboli e/o svantaggiate (come il **Codice Internet e Minori**).

La sicurezza deve essere declinata in un'ottica di "**total security**". Un'ottica che investe l'uso affidabile e consapevole della rete, la fiducia dell'utenza, le esigenze della *privacy*.

In questa visione entrano risvolti etici, industriali, tecnici che chiamano in causa i valori delle responsabilità e dell'uso razionale delle tecnologie.

Ma su questi temi tornerò nel corso del mio intervento.

Passo ora la parola al primo relatore del nostro dibattito.

Intervento

Riprendendo alcuni spunti da me suggeriti nell'intervento introduttivo, vorrei richiamare la vostra attenzione su alcuni fatti salienti , ai fini delle nostre considerazioni.

1) - Nella competizione internazionale dei mercati, le **reti** di comunicazione sono destinate a svolgere un **ruolo di primo piano**.

Se in alcuni Paesi – e l'Italia è fra questi – si stima per gli anni a venire una diminuzione delle linee di telefonia fissa, in altri si passerà direttamente dalla mancanza di collegamenti di tlc al cellulare, oppure a sistemi in cui il satellite si combina con il *wireless*.

2) – Le **piccole e medie imprese** che costituiscono l'ossatura del nostro sistema produttivo e molti fra **i distretti italiani sono in crisi** perché fanno fatica a reggere la concorrenza internazionale, a cominciare da quella cinese.

Molte imprese oggi scelgono la delocalizzazione, ma mantenendo nel nostro Paese gli *asset* aziendali considerati strategici (la direzione aziendale, il *marketing* ecc).

3) – Lo sviluppo delle **tecnologie di rete e la banda larga** sono ormai considerate un elemento capace di trasformare ogni Paese in un Paese competitivo.

In particolare, in Italia i distretti, attraverso la banda larga, possono dare vita ad **aziende estese** realizzando modelli di sviluppo che possono rilanciare ruolo e capacità organizzative.

4) – Lo sviluppo delle tecnologie ICT rappresenta una leva strategica per l'innovazione del Paese e per costruire in ogni campo della società e dell'economia - dall'*e-government* all'*e-business* e all'*e-commerce* - un **habitat di sviluppo per l'economia dei servizi**.

E potrei citare ancora altri elementi che riguardano le imprese ed il contesto in cui si trovano ad operare, ma per il momento mi limiterei a richiamarne solo un altro: la **sicurezza come presupposto trasversale** riferito a funzioni, procedure e infrastrutture con le quali devono confrontarsi le imprese medesime.

La sicurezza rappresenta la **condizione di base** per supportare e stimolare la crescente apertura in rete dei sistemi informativi, attraverso l'utilizzo della larga banda, dei servizi mobili e *wireless* di nuova generazione, dei portali, di *Intranet* e *Extranet*.

Vi è una consapevolezza sull'importanza di questo tema molto diffusa nelle **aziende sopra i 250 dipendenti** che, per la quasi totalità, ha già adottato più di un sistema di sicurezza informatica, come ci dicono i dati emersi dall'**Osservatorio permanente della Società dell'Informazione realizzato da Federcomin** (insieme al DIT).

Nelle aziende la cui fascia dimensionale va da 50 a 250 dipendenti la percentuale si colloca al **77%**.

Più scoperte sembrano essere le **realità di piccole dimensioni**, quelle che hanno da 1 a 9 dipendenti, che solo nel **22%** dei casi dispongono già di **almeno due sistemi di sicurezza informatica**.

Ciò sembra dovuto sia al **minore livello di informatizzazione** e di utilizzo di Internet rispetto alle aziende di maggiori dimensioni, sia alla **relativa semplicità della loro dotazione informatica** che nella maggior parte dei casi può essere protetta anche solo da un sistema antivirus.

Gli **antivirus** rimangono infatti i sistemi di sicurezza **più diffusi tra le aziende italiane**. Questa soluzione viene citata dalle aziende con la frequenza più elevata, sia quando si considerano i **nuovi investimenti** che gli **aggiornamenti delle soluzioni esistenti** effettuati negli ultimi tre mesi prima dell'indagine.

Un'altra area nella quale si concentrano gli investimenti in sicurezza è rappresentata dai **firewall**, a conferma dell'importanza degli aspetti di difesa da attacchi e intrusioni dall'esterno, mentre **soluzioni più evolute** (es. autenticazione accessi, crittografia ecc.) coinvolgono un **numero ancora limitato di aziende**, analogamente a quanto accade per l'utilizzo di un *back-up* dei dati localizzato all'esterno della sede aziendale.

Quest'ultimo dato è la spia di un **approccio delle aziende italiane ancora poco attento al valore delle informazioni e delle applicazioni utilizzate**.

Infatti solo nelle strutture di maggiori dimensioni le informazioni vengono generalmente duplicate per affrontare eventuali "*black out*" dei sistemi informativi, ricorrendo a servizi di ripartenza localizzati all'esterno dell'azienda, presso centri correttamente attrezzati per la gestione di emergenze.

Questo **approccio "parzialmente evoluto"** alla gestione della sicurezza può essere anche spiegato con la percezione rilevata

presso le aziende italiane dei pericoli informatici a cui sono state esposte nell'ultimo anno. Infatti solo una percentuale oscillante tra il **20 e il 30%** delle aziende con accesso a Internet ritiene di avere avuto problemi di sicurezza informatica negli ultimi 12 mesi.

Anche la **maggior parte degli utilizzatori Internet da casa (64%)** si è dotato di misure di sicurezza per proteggere il *computer*.

Gli aggiornamenti di questi *software* vengono eseguiti direttamente da persone della famiglia (nel **70%** dei casi), solo il **14%** degli utilizzatori ricorre ad un tecnico.

La sensibilità verso un **utilizzo consapevole del mezzo Internet** è andata crescendo negli ultimi anni, parallelamente a un incremento della sua diffusione nelle case e negli uffici degli italiani.

La consapevolezza dei potenziali rischi genera frequentemente un atteggiamento di attenzione da parte del navigatore nei confronti dei contenuti che la rete gli propone.

Dei **19,4 milioni di utilizzatori Internet** (sempre secondo i dati emersi dall'**Osservatorio Federcomin**) il **56,7%** dichiara di prestare sempre molta attenzione agli indirizzi digitati nella barra del *browser* e a certa pubblicità che compare sulle pagine *web*. Il **29,2%** alza il livello di attenzione solo sui siti mai frequentati in precedenza. Solo il **14,1%** non è particolarmente allarmato quando naviga.

Il quadro che emerge da un **primo bilancio** sull'andamento del **settore ICT** nell'anno appena trascorso contiene **luci e ombre**. I segnali di ottimismo che provengono dallo sviluppo delle telecomunicazioni mobili e dalla diffusione dei servizi di base nelle famiglie e nelle PA si contrappongono alla modestia degli investimenti IT nelle imprese (soprattutto nelle PMI) e all'insufficiente utilizzo di tecnologie a scopi educativi e commerciali.

Secondo i **dati di EITO**, dopo un biennio di contrazione degli investimenti in IT nel nostro Paese, il 2004 dovrebbe segnare un risultato di sostanziale pareggio (la stima è pari **+0,6%**) con una ripresa più sensibile nel 2005, stimata nel **3,3%**).

Nell'ambito dell'IT, il segmento della sicurezza è sicuramente quello che registra investimenti più vivaci da parte delle imprese.

E' assolutamente necessario superare l'idea e la cultura che la sicurezza rappresenti un "costo" da sostenere e quindi da evitare.

Occorre ribaltare questa impostazione riduttiva portando le imprese, i cittadini, le Pubbliche amministrazioni a considerare la sicurezza come un **"investimento" in qualità e fiducia per gli utenti**: una componente, pertanto, in grado di esaltare i benefici delle tecnologie ICT.

Federcomin ritiene che la prima azione da condurre per la sicurezza sia quella della **prevenzione** e quindi quella che considera come determinanti:

- un **approccio sistematico** che affronti il problema in maniera strutturata e non episodica;

- **gli aspetti dell'informazione e della formazione** (a partire da quella scolastica e professionale) anche attraverso opportuni Programmi di sensibilizzazione e di formazione delle aziende, delle Pubbliche Amministrazioni e dei cittadini sui rischi e sulle soluzioni disponibili;
- **la diffusione di strumenti ed architetture di sicurezza** dei sistemi informatici e telematici;
- **la promozione di Servizi di Assistenza** gestita a tempo pieno da parte di Centri Operativi Certificati, per la sicurezza al fine di sopperire alle carenze strutturali della realtà italiana. Non basta approntare misure e sistemi di sicurezza, serve utilizzarli correttamente mantenendoli attivi ed aggiornati;
- **i sistemi di autoregolamentazione;**
- **l'uso affidabile di reti, servizi ed applicazioni** attraverso la definizione di *standard* di sicurezza e sistemi di certificazione che dovranno essere sviluppati a largo spettro;

- la **promozione di progetti di ricerca per la sicurezza** che seguano l'evoluzione della problematica con una velocità almeno pari allo sviluppo tecnologico.

L'approccio verso l'uso di tali strumenti ed architetture dovrà essere di tipo "**globale**", garantendo un ambiente complessivamente sicuro con tecnologie di facile implementazione ed utilizzazione "integrata" e dovrà essere anche la risposta che le Istituzioni daranno al problema considerandone tutti gli aspetti e le competenze.

Rimane poi centrale, in ogni sistema ICT in cui **sicurezza è sinonimo di affidabilità**, la figura di un **ICT Security manager** aziendale, una nuova figura che ogni impresa dovrebbe considerare irrinunciabile.

Le aziende dovranno definire politiche imprenditoriali che inquadrino la sicurezza in un contesto generale di difesa dell'azienda, in ogni suo aspetto ed attività.

Ciò richiede, com'è evidente, una **vision** ampia nella strategia di impresa, ma anche la capacità di **destinare alla sicurezza investimenti sicuramente più significativi di quelli attuali.**

Perché la sicurezza rimane un asset imprescindibile.

E su questa consapevolezza occorre stabilire un "comune sentire ed operare" per lo sviluppo dell'ICT.