

## Sicurezza informatica e utilizzo dei computer in azienda un'indagine SUPSI nella realtà della Svizzera italiana

Silvano Marioni, CISSP

SUPSI – Dipartimento Tecnologie Innovative

ISIN – ISSI

Galleria 2, CH-6928 Manno

tel. 058 666 65 78 - fax 058 666 65 71

e-mail: [silvano.marioni@supsi.ch](mailto:silvano.marioni@supsi.ch)

sito web: [www.dti.supsi.ch](http://www.dti.supsi.ch)



## Perché un'indagine sulla sicurezza

- Per capire cosa fanno le aziende della Svizzera italiana per la protezione dei loro dati aziendali e dei loro sistemi informativi
  - Quali sono i dati aziendali e quanto vengono considerati critici
  - Quali sono le misure tecniche e organizzative previste
  - Quale è il ruolo dei dipendenti
- Per capire le specificità della realtà locale rispetto a quanto ci propone la scena globale
  - Quale è la sensibilità locale rispetto al tema della sicurezza
  - Come vengono affrontati e risolti i vari aspetti della sicurezza



## Come si è svolta l'indagine

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

- I dati sono stati raccolti con un formulario con 19 domande
  - Da compilare direttamente su Internet
  - Oppure da compilare e spedire
- Sono state contattate circa 2'500 aziende direttamente dalla SUPSI o tramite associazioni o organizzazioni di categoria
- Non è stata fatta volutamente una campionatura e si sono considerate le risposte come un elemento per valutare la sensibilità al tema della sicurezza
- La raccolta dati è durata da settembre a novembre 2006
- I dati sono disponibili all'indirizzo [www.dti.supsi.ch/isis](http://www.dti.supsi.ch/isis)

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 3 -

ISIN - Sistemi Informativi e Networking



## I settori di attività dell'inchiesta

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

- Le associazioni e organizzazioni di categoria che hanno collaborato all'inchiesta sono state:
  - Associazione fabbricanti ramo abbigliamento del Cantone Ticino
  - Associazione Industrie Ticinesi
  - Associazione installatori elettricisti ticinesi
  - Centro Studi Bancari
  - Camera di commercio, dell'industria e dell'artigianato del Cantone Ticino
  - CLUSIS, Associazione svizzera della sicurezza dei sistemi d'informazione
  - Dauf SA
  - Istituto di formazione delle professioni fiduciarie
  - Ordine degli Avvocati del Canton Ticino
  - Ordine dei medici del Canton Ticino
  - Ordine dei notai del Cantone Ticino
  - Sezione degli enti locali del Cantone Ticino
  - Società Svizzera Impresari Costruttori, Sezione Ticino
  - Unione professionale svizzera dell'automobile, Sezione Ticino

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 4 -

ISIN - Sistemi Informativi e Networking



## Chi ha risposto all'inchiesta

- Si sono avute 355 risposte
  - 257 tramite Internet, 98 in forma cartacea
  - 39 in forma anonima, 316 con nominativo
  
- Confronto con altre inchieste sul tema della sicurezza
  - Computer Crime and Security Survey 2006, CSI/FBI, dati forniti da 616 responsabili della sicurezza in azienda,
  - Sicurezza dell'informazione nelle imprese svizzere, agosto 2006, CSS/ETH, invii/risposte 5000/562



## Un'ulteriore strumento di analisi



### Sicurezza Informatica e utilizzo dei computer in azienda - analisi dinamica dei dati

Questa pagina permette di esaminare in modo dinamico le risposte dell'inchiesta, sia direttamente per ogni domanda, sia confrontando in modo incrociato le differenti domande tra loro.  
Per ulteriori informazioni sull'inchiesta si rimanda al documento "Sicurezza informatica e utilizzo dei computer in azienda"



**Legenda**

- Nessun server
- Tra uno e cinque
- Più di cinque

Percentuale relativa alla categoria di risposta  
 Percentuale relativa al totale delle risposte

	Meno di cinque PC	%	Tra cinque e venti	%	Tra venti e cento	%	Più di cento	%
Nessun server	28	81.78	9	6.87	0	0	1	1.34
Tra uno e cinque	34	48.22	122	83.13	34	78	2	7.81
Più di cinque	0	0	0	0	12	28	58	80.63
Totale risposte	112	100	131	100	48	100	64	100



## Presentazione dei risultati



## Risposte suddivise per numero di PC

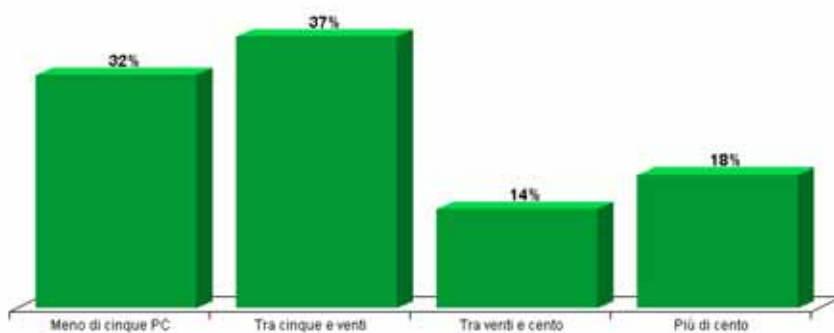


Figura 2 : percentuale di aziende per numero di PC



## Risposte suddivise per settori di attività

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana

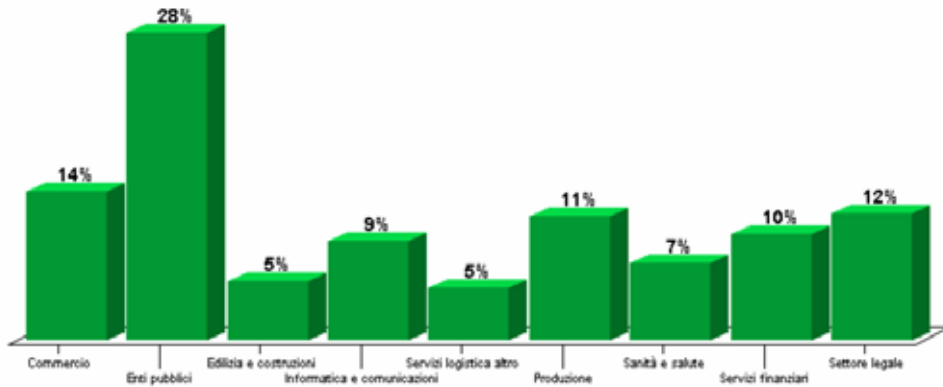


Figura 2 : percentuale di aziende per settore di attività



## Informazioni critiche memorizzate

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana

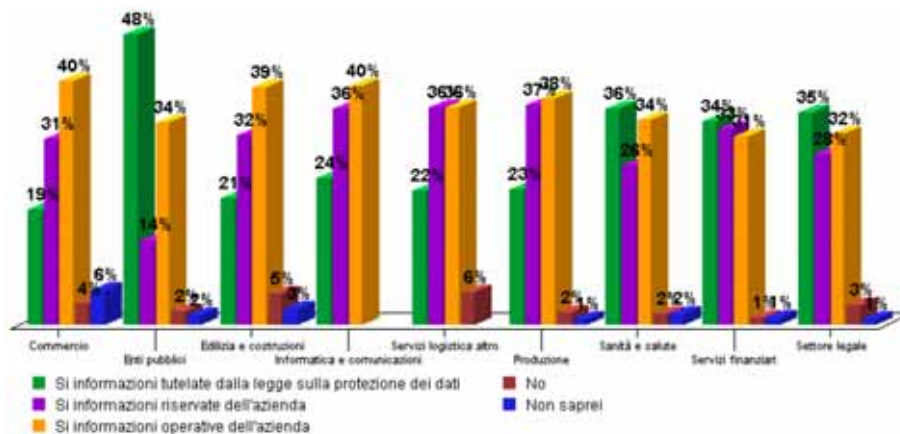


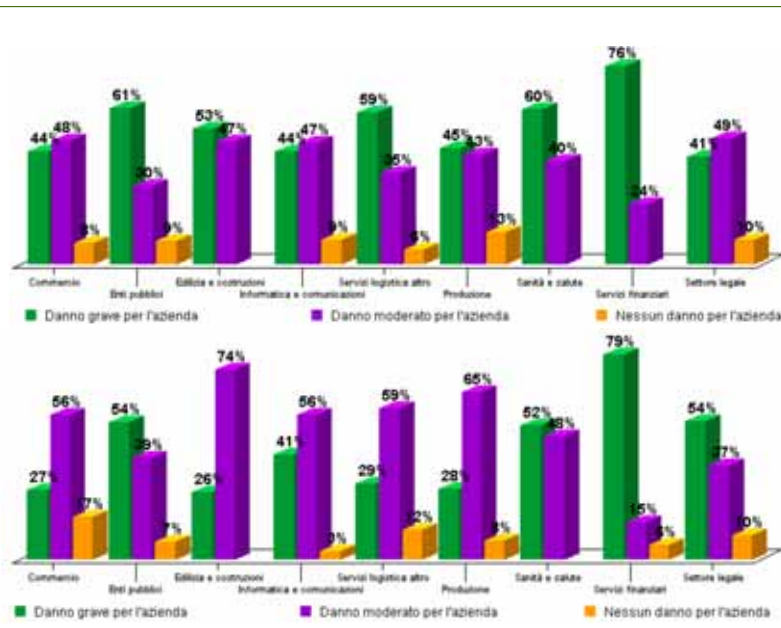
Figura 14 : percentuale di informazioni critiche sui PC e sui server aziendali suddivisa per settore di attività



## Danni alle informazioni aziendali

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana



Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 11 -

ISIN - Sistemi Informativi e Networking

## Utilizzo di Internet

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana

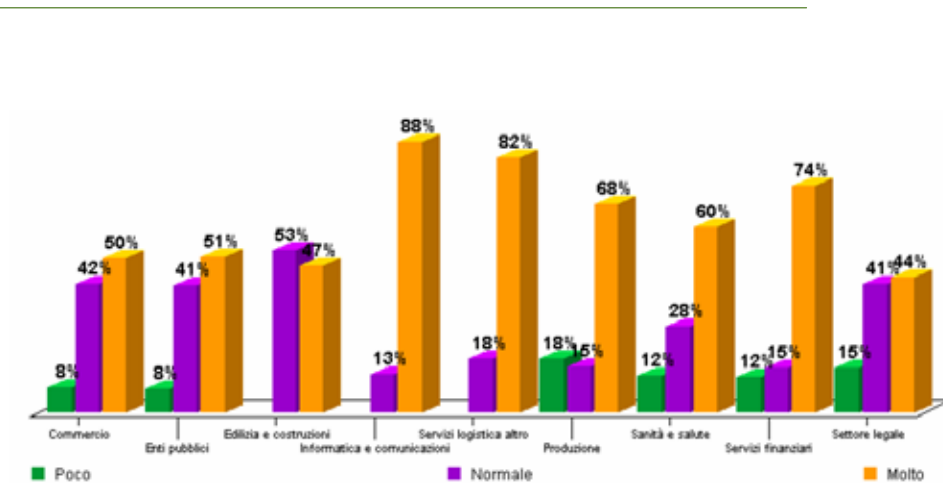


Figura 6 : percentuale di utilizzo della rete Internet per la posta elettronica suddivisa per settore di attività

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 12 -

ISIN - Sistemi Informativi e Networking

## Gravità nell'uso improprio di Internet

SUPSI  
Scuola Universitaria Professionale  
della Svizzera Italiana

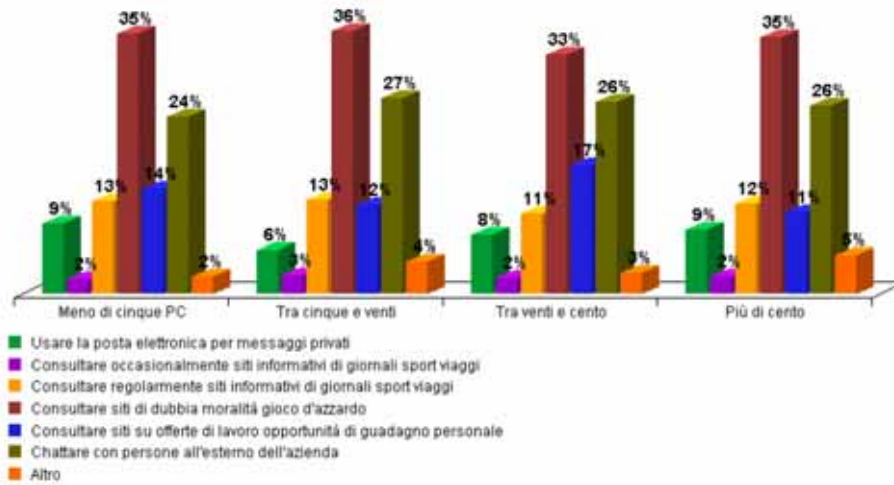


Figura 26 : percentuale delle attività ritenute gravi nell'utilizzo di Internet da parte dei dipendenti suddivisa per dimensioni



Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 13 -

ISIN - Sistemi Informativi e Networking

## Necessità di controllo dei dipendenti

SUPSI  
Scuola Universitaria Professionale  
della Svizzera Italiana

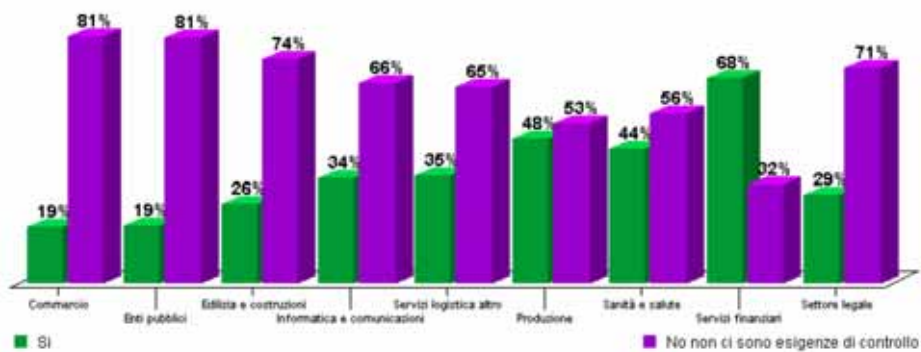


Figura 23 : percentuale sulle esigenze di controllo dei dipendenti nell'uso dei PC e di Internet suddivisa per settore di attività



Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 14 -

ISIN - Sistemi Informativi e Networking

## Analisi di alcuni risultati



## Posta elettronica

- Sistema di comunicazione capillare, rapido e economico
- Limiti tecnologici
  - Il testo del messaggio è in chiaro
  - Il mittente può essere alterato
  - Non si conosce il percorso del messaggio
- Cattive abitudini consolidate
  - Diffusione di messaggi personali « giocosi »
  - Invio documenti importanti per posta elettronica
- Rischi
  - Occupazione impropria dello spazio disco aziendale
  - Possibile diffusione di programmi malefici
  - Possibili furti di informazioni importanti



## Uso della posta elettronica

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

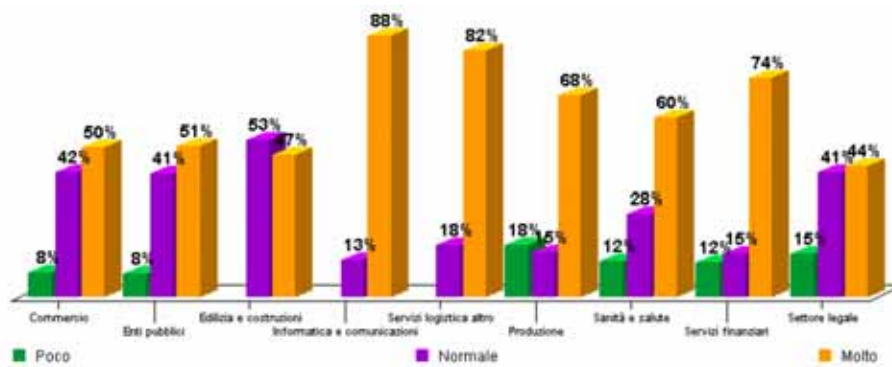


Figura 6: percentuale di utilizzo della rete Internet per la posta elettronica suddivisa per settore di attività

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 17 -

ISIN - Sistemi Informativi e Networking



## Uso della posta elettronica

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

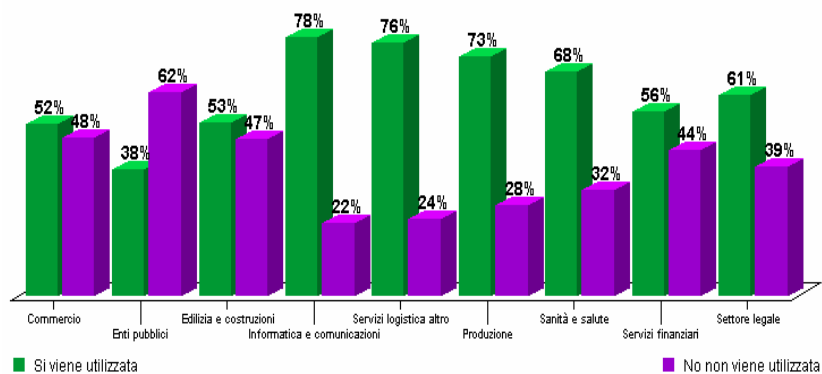


Figura 20: percentuale di utilizzo della posta elettronica per inviare e/o ricevere documenti aziendali importanti suddivisa per settore di attività

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 18 -

ISIN - Sistemi Informativi e Networking



## Accesso al sistema informatico

- Autenticarsi sul sistema informatico per essere autorizzato a svolgere una determinata attività
- Limiti tecnologici
  - È possibile non autenticarsi (non usare la password di accesso)
  - Nessun contesto operativo diverso tra utente amministratore e utente normale
  - Alcune applicazioni richiedono l'utente amministratore
- Cattive abitudini consolidate
  - Non usare la password o usare una password deboli (o sul bigliettino)
  - Lavorare come utente amministratore
- Rischi
  - Accesso al sistema informatico da parte di terzi
  - Maggiore vulnerabilità ai codici malefici



## Misure tecniche di sicurezza

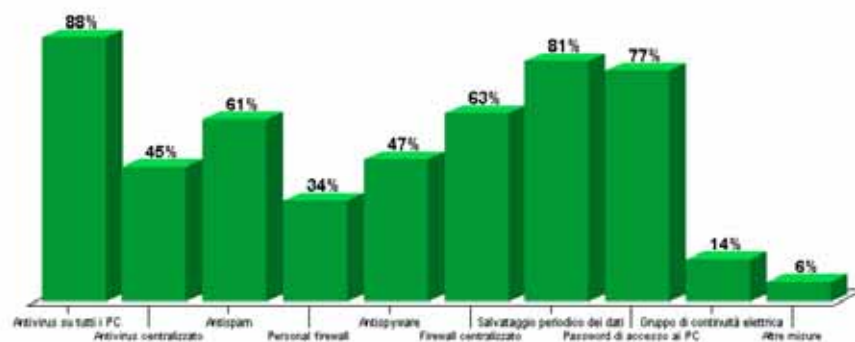


Figura 29 : percentuale delle misure tecniche previste per l'infrastruttura informatica aziendale  
(Il totale della percentuale supera il 100% perché la domanda permetteva scelte multiple)



## I comportamenti per la sicurezza

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

- Conoscere
  - Essere a **conoscenza** e **consapevoli** dei rischi che si possono incontrare
- Capire
  - Saper **riconoscere** le situazioni critiche a rischio
- Reagire
  - Decidere il tipo di **reazione** secondo la situazione
- Diventano importanti
  - I regolamenti
  - La formazione del personale



Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 21 -

ISIN – Sistemi Informativi e Networking

## Regolamenti per settore

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

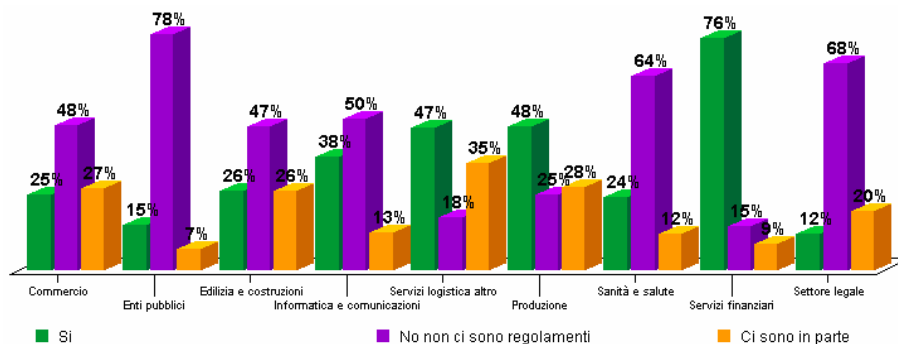


Figura 27 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per settore di attività



Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 22 -

ISIN – Sistemi Informativi e Networking

## Regolamenti per dimensione

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana

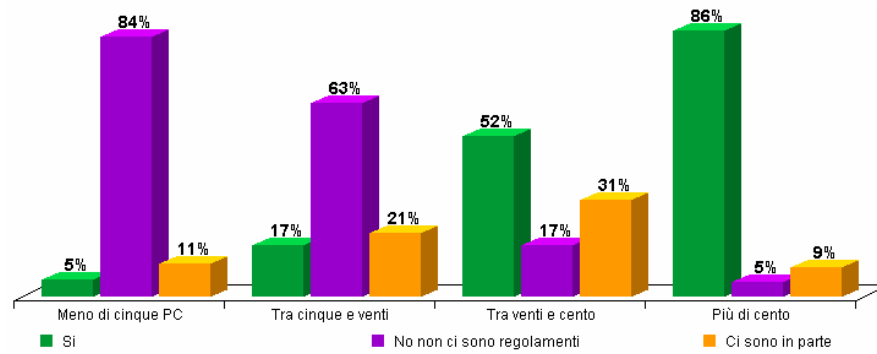


Figura 28 : percentuale di aziende con regolamenti che disciplinano l'uso dei PC e di Internet da parte dei dipendenti suddivisa per dimensioni

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 23 -

ISIN - Sistemi Informativi e Networking



## Competenze per settore

SUPSI

Scuola Universitaria Professionale della Svizzera Italiana

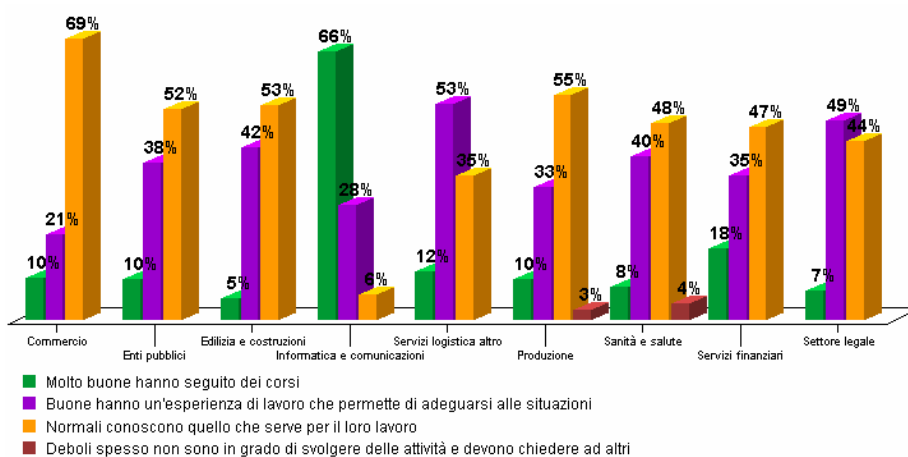


Figura 22 : percentuale sulle competenze dei dipendenti sull'uso dei PC e di Internet suddivisa per settore di attività

Ticino Informatica, 25 ottobre 2007, Silvano Marioni

- 24 -

ISIN - Sistemi Informativi e Networking



## Conclusioni

SUPSI

Scuola Universitaria Professionale  
della Svizzera Italiana

- Le aziende hanno gran parte dei dati aziendali critici su supporti informatici e sono coscienti dei vantaggi attuali e futuri dell'informatica
- C'è la consapevolezza dei danni che possono derivare dalla distruzione o dal furto dei dati informatici aziendali
- È meno forte la consapevolezza sulla necessità di comportamenti orientati alla sicurezza come ad esempio nel caso della posta elettronica
- In generale mancano regolamenti per sensibilizzare e indicare i comportamenti corretti ai dipendenti, ma soprattutto per tutelare l'azienda in caso di problemi
- Tranne casi specifici, la formazione dei dipendenti non viene considerata fondamentale per l'utilizzo e la sicurezza dei dati aziendali



«Always remember:  
Amateurs hack systems.  
Professionals hack people»

Bruce Schneier

