

LA SICUREZZA DELLE INFORMAZIONI
IN UNA ORGANIZZAZIONE SANITARIA:
OBBLIGO O STRATEGIA? Bologna 16 giugno 2006



LA TUTELA DEL PATRIMONIO INFORMATIVO IN UNA ORGANIZZAZIONE SANITARIA



Ing. Nico Mastrorillo (Direttore Affari Esteri e Comunicazione CERMET)
La tutela del patrimonio informativo in una organizzazione sanitaria

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

☞ Le **informazioni** nel moderno tessuto socio economico rappresentano **una componente strategica cruciale** ai fini del successo delle iniziative aziendali.

Un noto top manager ha detto, sintetizzando un intuitivo buon senso, *che “... l'importante è avere le informazioni giuste, al momento giusto, e saperle gestire in modo appropriato”*.

☞ Ne consegue che questa risorsa dovrebbe essere **tutelata** come tutte quelle strategiche per l'azienda...

Le informazioni aziendali assumono differenti forme:

- ⇒ Archivi elettronici
- ⇒ Trasmissione elettronica
- ⇒ Carta
- ⇒ Nastro magnetico/CD/DVD
- ⇒ Microfilm
- ⇒ Conversazioni telefoniche o “de visu”

Ogni forma comporta rischi specifici..

! Non esistono informazioni esenti da rischi !

- ☞ **Le informazioni aziendali di tipo elettronico** cominciano ad essere **la parte maggiore e più critica del capitale societario** ed insieme al capitale umano costituiscono **l'ossatura della azienda, la sua garanzia di solidità** (anche se le info aziendali contemplano anche ed ancora altri supporti)
- ☞ Ciò è tanto più vero quanto più le aziende utilizzano sistemi di comunicazione aperti all'esterno e basati sulla rete web

Le seguenti **caratteristiche** diventano pertanto **essenziali** ai fini della corretta gestione sistematica delle Informazioni (**SGSI**):

- ! **CONFIDENZIALITÀ:** solo gli utenti autorizzati possono accedere alle informazioni pertinenti
- ! **INTEGRITÀ:** protezione contro danneggiamenti o modifiche, dolose o involontarie
- ! **DISPONIBILITÀ:** le informazioni sono rese disponibili on demand e in modo appropriato

LA SICUREZZA DELLE INFORMAZIONI
 IN UNA ORGANIZZAZIONE SANITARIA:
 OBBLIGO O STRATEGIA? Bologna 16 giugno 2006



ALTA				
MEDIO ALTA				
MEDIO BASSA				
MOLTO BASSA				
	TRASCURABILE	MODESTA	NOTEVOLE	ELEVATA

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani



Ing. Nico Mastrorillo (Direttore Affari Esteri e Comunicazione CERMET)
 La tutela del patrimonio informativo in una organizzazione sanitaria

LA SICUREZZA DELLE INFORMAZIONI
IN UNA ORGANIZZAZIONE SANITARIA:
OBBLIGO O STRATEGIA? Bologna 16 giugno 2006



CERMET-WE CARE FORUM e AIOP

**Indagine sulla Gestione della Sicurezza del Patrimonio
informativo nella Vostra Struttura sanitaria**



IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani



Ing. Nico Mastrorillo (Direttore Affari Esteri e Comunicazione CERMET)
La tutela del patrimonio informativo in una organizzazione sanitaria

**STATUS DELL'INFORMATION
SECURITY NELLE STRUTTURE
SANITARIE PUBBLICHE E PRIVATE**





Una piattaforma web (www.zoomerang.com)
attraverso cui è possibile inviare questionari di
indagine, costruiti e personalizzati da nelle domande e
nella grafica.

La piattaforma stessa elabora le risposte e aggrega i
risultati.




Per l'invio è stato creato un apposito indirizzo di posta
elettronica customercare@cermet.it.

**RISULTATI DELL'INDAGINE
AIOP – WE CARE FORUM
sullo status dell'Information Security
nelle strutture sanitarie**




Campione dell'indagine

Soci CERMET – WE CARE FORUM
Soci AIOP dell'Emilia Romagna




Di cui, la percentuale di risposta

Aiop		25%
We Care Forum		42%
Entrambi		33%




All'interno della Vostra struttura , nel **budget di spesa annuale** viene riservata una voce alla gestione della sicurezza del patrimonio informativo?

Sì		25%
No		17%
Parzialmente		58%




All'interno della Vostra struttura è stato **incaricato un responsabile** per la gestione della sicurezza del patrimonio informativo?

Sì		75%
No		8%
Parzialmente		17%



Viene gestita una **periodica attività formativa sul personale** relativamente alle problematiche che impattano sulla sicurezza delle informazioni e sugli aggiornamenti normativi (ed esempio la Legge sulla Privacy)?

Sì		67%
No		17%
Parzialmente		17%




sono stati **informati/formati i fornitori principali** (società di pulizie, manutentori, ecc.) sulle principali criticità relative alla sicurezza delle informazioni e sui comportamenti più idonei da tenere in materia (ad es. identificazione visibile, procedure di sicurezza, segnalazione potenziali criticità alla sicurezza ecc.)?

Sì		33%
No		33%
Parzialmente		33%

E' stata formalmente **incaricata una persona per la gestione dei back-up** (sia delle macchine comuni – ad es. server – sia delle macchine ad uso dei professionisti - ad es. i portatili)?
Il back up viene gestito secondo una procedura definita e validata?

Sì		75%
No		25%
Parzialmente		0%



Viene fatta un opera di informazione o di **controllo sul software installato in autonomia** dal personale sui propri PC (applicativi FREE scaricati da Internet, utilità allegate a riviste o a dispositivi hardware come dizionari, software per la gestione di macchine digitali, ecc.).

Sì		58%
No		25%
Parzialmente		17%




LA SICUREZZA DELLE INFORMAZIONI IN UNA ORGANIZZAZIONE SANITARIA: OBBLIGO O STRATEGIA? Bologna 16 giugno 2006






Viene fatta un'opera di **informazione o di controllo su eventuali virus, worm, trojan, spyware ecc.** che potrebbero essere eventualmente installati sui PC?

Sì		83%
No		17%
Parzialmente		0%




E' stato definito un **Business Continuity Plan (Piano della Continuità Operativa)** da attivare in caso di eventi/incidenti di rilievo (ad es. black-out, incendio, allagamento ecc.) ?

Sì		42%
No		25%
Parzialmente		33%




Viene fatta un'opera di informazione sulla opportunità di **non lasciare** documenti, fogli, post-it contenenti **informazioni riservate sulla scrivania** soprattutto nei momenti di assenza (**Clear Desk Policy**)?

Sì		67%
No		17%
Parzialmente		17%

Nei momenti in cui la postazione di lavoro risulta sguarnita, è stato introdotto un **automatismo che blocchi** la possibilità di utilizzare il Personal computer (**screen saver con password**)?

Sì		50%
No		17%
Parzialmente		33%

viene fatta un'opera di informazione sulla opportunità di **eliminare tutti i dati** all'interno di un Personal Computer ma anche solo di un dischetto, una chiavetta USB, un CD-Rom, un DvD prima della sua dismissione/eliminazione?

Sì		58%
No		17%
Parzialmente		25%