

# Sicurezza fisica e sicurezza logica: due culture si incontrano

---

*L. Vann.*

Sicurezza fisica  
e sicurezza logica:  
due culture si incontrano ?

*La "Cultura della Sicurezza"*

*Trae origine*

*Dall'incontro tra l'Uomo ed il Cane*

*(non si sa chi dei due abbia avuto l'iniziativa)*

---

*L. Vann.*

## *Sicurezza FISICA ....*



---

*L. Vann.*

*... anche "INTERNA" ...*



---

*L. Vann.*

*... FIREWALLING...*



---

*L. Vann.*

*... magari anche "LOGICA" ...*



---

*L. Vann.*

Sicurezza fisica  
e sicurezza logica:  
due culture si incontrano !



# La Sicurezza nei Contratti ICT

“Che cosa il Committente può *ragionevolmente*  
pretendere

Che cosa il Fornitore deve *ragionevolmente*  
garantire”

## In quali Contratti ?

tutti quelli in cui siano previste le seguenti facoltà

- Accesso (fisico o virtuale / remoto)
  - Permanenza / intromissione in applicazioni
  - Sviluppo / personalizzazioni, ecc.
  - Interventi in aree protette (fisiche o virtuali)
- 
- Durata del rapporto contrattuale

*...praticamente, tutti i contratti di:*

- Manutenzione (HW, SW o impianti)
- Assistenza, consulenza
- Sviluppo, personalizzazione applicazioni
- Gestione continuativa di applicazioni
- Outsourcing di processi (di qualunque genere)

## Sicurezza FISICA : *cosa vuol dire ?*

- accesso aree
  - protezione supporti
  - prevenzione incidenti (incendio, ecc.)
  - separazione fisica supporti / data base
  - archivi fisici separati e protetti
  - back-up / recovery
- ... eccetera ...

## Sicurezza LOGICA: *cosa vuol dire ?*

- barriere SW di protezione
  - chiavi accesso per livelli / log / identificativi
  - encryption / firme digitali, ecc.
  - antivirus (e simili...)
  - monitoring saltuari e periodici
  - "intrusion detection"
- ... eccetera ...

... per i CONTRATTI ...

Due Definizioni: *(al solo scopo di questa presentazione)*

❖ DATI: sequenze alfanumeriche suscettibili di elaborazione

❖ INFORMAZIONI: insieme aggregato di dati che dà a chi ne accede una notizia aggiuntiva

*ESEMPI .....*

---

**L. Vann.**

## I DATI, in quanto tali, devono essere:

- memorizzabili, reperibili, gestibili
- protetti da perdite – fortuite o dolose
- accessibili solo dagli autorizzati
- recuperabili, in caso di “crash”
- protetti “in itinere” = in fase di trasmissione
- gestibili, modificabili solo dagli autorizzati (diversi livelli di autorizzazioni)

In sede di definizione contrattuale, ne consegue che:

- II COMMITTENTE deve  
fissare le sue policy e specs di sicurezza (sia fisica che logica)  
fissare i perimetri di azione del Fornitore – sia fisici che logici – e controllarne l’osservanza  
comunicare tutte le info pertinenti
- II FORNITORE deve  
adempiere a tutto quanto sopra  
*ruolo diverso se Fornitore di Sicurezza*

## Riservatezza delle INFORMAZIONI

Presupposto: le info da proteggere sono già in possesso o comunque accessibili / conoscibili

### Obiettivo del COMMITTENTE:

- impedirne l'uso improprio / divulgazione

### Obiettivo del FORNITORE:

- definire "quali", "come" e per quanto tempo
- assumere l'impegno e trasferirlo al personale
- mantenere il controllo

## Considerazioni

A) - Sicurezza e protezione dei DATI :

in PREVALENZA problema "tecnico" di pertinenza dello "owner" del sistema

il Committente può *pretendere* solo ciò che ha definito come specs - sia fisiche che logiche

il Fornitore può/deve *garantire* solo le obbligazioni definite e accettate a contratto

*... importanza della fase di negoziazione*

## Considerazioni

A) - Sicurezza e protezione dei DATI: *(segue)*

- contratti di sviluppo / adeguamento SW:  
adeguamento a specs *fisiche e logiche* esistenti
- contratti di Outs. / Gestione Security  
accordo su nuove implementazioni

Responsabilità: *accurata definizione contrattuale – normalmente il fornitore dell'antifurto non può essere responsabile se il ladro è stato più "bravo" salvo colpa grave*

## Considerazioni

### B) – Riservatezza delle INFORMAZIONI:

Regolamentazione contrattuale di  
*comportamenti umani*

definire “quali” info sono riservate  
*“tutto è riservato” equivale a “nulla...”*  
*stabilire almeno le “tematiche” – definire le*  
*esclusioni (es. info di dominio pubblico)*

definire “come”: Es. “...usando lo stesso grado  
di cura e discrezione impiegato per le proprie  
info riservate” – valido se certif. Qualità

## Considerazioni

B) – Riservatezza delle INFORMAZIONI:  
Regolamentazione contrattuale di  
*comportamenti umani (...segue)*

Il dilemma delle “definizioni”:

RISERVATEZZA = *accesso solo agli autorizzati*

CONFIDENZIALITA' = *non divulgazione a non aut.*

*... ma, quale il comportamento degli “autorizzati” ?*

*“Comportamenti Umani” = anello debole della catena...*

Classificazione dei livelli di riservatezza

Procedure / norme di gestione dei documenti

*... e dei comportamenti !*

## Considerazioni

### B) – Riservatezza delle INFORMAZIONI:

Regolamentazione contrattuale di  
*comportamenti umani (...segue)*

Trasferire validamente le obbligazioni al  
personale *proprio e dei subcontractors*

In casi particolari, procedure ad hoc per il  
trasferimento, detenzione e restituzione della  
documentazione

Stabilire un limite temporale (es.: 2 anni dopo  
il termine del contratto)

## Considerazioni

B) – Riservatezza delle INFORMAZIONI: *(segue)*

Frequente sovrapposizione con “Proprietà del SW” –  
due tematiche diverse e distinte  
*è opportuno differenziarle in contratto ...*

Il problema dei “Residuals”:

*“... le idee, concetti, know-how o tecniche relativi alla  
elaborazione e trasmissione dei dati potranno essere usati da  
entrambe le parti, senza limitazione alcuna”*

principio riconosciuto anche dalla legge

*(art. 2 Dlgs 518 / 92 “tutela del SW”)*

*“...non si può lobotomizzare il sistemista...”*

Alcune conclusioni ...

Disponibilità vs Riservatezza = *il dilemma insoluto* ...

Rapporto contrattuale = *necessaria intromissione di una delle parti nella "intimità" dell'altra*

Clausole di salvaguardia:

- ✓ *per i DATI, OK se le specs sono esaurienti*
- ✓ *per le INFO, relatività e "limiti" del rapporto umano*

Sicurezza FISICA e S. LOGICA = *solo se integrate contribuiscono validamente a limitare i rischi*

Alcune conclusioni ...

## NEGOZIAZIONE del Contratto

valutare il rischio "Sicurezza"

monitoring degli accessi alla controparte  
*"need to know"*

vincoli "tecnici" – specs fisiche e logiche  
= *"come pretendo che si lavori..."*  
*procedure interne come "manuale"*

INFO: *rilasciare solo quelle indispensabili*  
*segreto profess. = OK solo per det. Professioni*  
*"Lettere di non disclosure"*

---

**L. Vann.**

*... e quindi →*

*“ Requisiti per una BUONA NEGOZIAZIONE”*

- *visione di insieme*
- *valutazione dei rischi (... “tutti”...)*
- *priorità*
- *analisi / scelte ponderate*
- *“partnership” = preconstituire un clima favorevole a rinegoziazioni*



*Grazie per la vostra attenzione !*

Luigi Vannutelli – e-mail: [luigi.vannutelli@sercit.com](mailto:luigi.vannutelli@sercit.com)

---

**L. Vann.**