



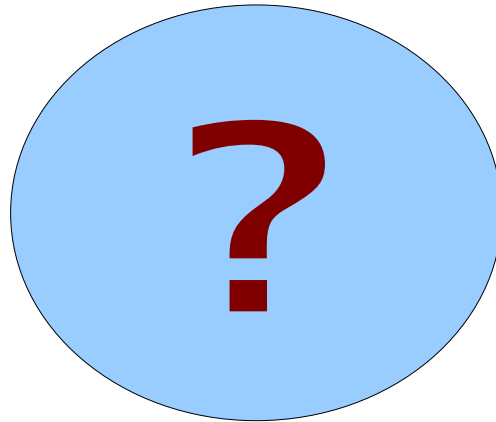
L'OUTSOURCING IT: BEST PRACTICE E AUDITING

La Sicurezza e gli SLA

*Andrea Pasquinucci, PhD CISA CISSP
UCCI.IT*

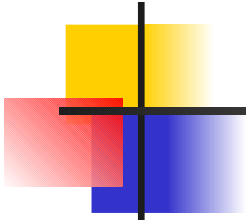


Outsourcing



Sicurezza

Contratto





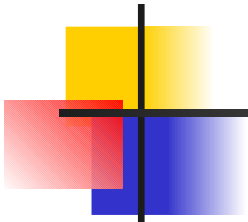
Sicurezza

- Conoscere i propri sistemi
- Conoscere i propri dati/informazioni
- Conoscere i propri utenti

- Politiche, Linee Guida, Procedure, Istruzioni Operative ...



Controlli





Sicurezza e Outsourcing



- **Non** conosciamo i sistemi
- Conosciamo i dati/informazioni
- Conosciamo gli utenti
- **Non** conosciamo gli amministratori ICT
- **Non** gestiamo i sistemi ICT



Sicurezza e Outsourcing

- Abbiamo Politiche ecc.
- Ma i sistemi ICT sono gestiti con **altre** Politiche ecc.
- **Gestione, controllo e verifica** dei sistemi ICT sono fatti dal Fornitore
- *Ma i dati sono del Cliente!*



Sicurezza e Outsourcing



Esempio:

- Imporre Politiche di accesso ai dati
 - Sapere chi ha avuto accesso ai dati
 - Anche tra gli amministratori di sistema
 - Report delle violazioni
 - ...
- Senza avere controllo ne accesso amministrativo ai sistemi → Come ?



Outsourcing

Come fare:

- *Ottenere accesso amministrativo ai sistemi*
- Non ha senso:
 - Il Cliente deve mantenere gli amministratori di sistema come se avesse il sistema in casa
 - Il Fornitore condivide le risorse tra più clienti e non può permettere ai tutti i clienti di controllare i propri sistemi
 - Ogni Cliente ha Politiche diverse



Il Contratto

Specificare nel contratto:

- Non solo le funzionalità richieste
- **Anche i controlli e le Politiche da implementare**
- Il Fornitore deve avere Politiche generali che garantiscano il rispetto di quelle dei Clienti
 - Certificazioni internazionali (ISO, SAS70 ecc.) aiutano ma non sono sufficienti



Il Contratto

Attenzione:

- ICT cambia molto *rapidamente*
- Le implementazioni delle Politiche cambiano altrettanto rapidamente
- **Il contratto, negli allegati tecnici, deve cambiare altrettanto rapidamente e frequentemente!**



Problema

Come fare a **verificare** che le politiche del Cliente siano correttamente implementate dal Fornitore ?

- Il Cliente ha il diritto (in prima persona o tramite terzi) di eseguire verifiche (*audit*) sul Fornitore
 - Di solito è utile ma non è sufficiente
- **Service Level Agreement (SLA)**



SLA



Gli SLA sono il **cardine** per il **Controllo** da parte del Cliente sui servizi offerti dal Fornitore:

- Descrizione tecnica dettagliata dei servizi
- Garanzie sulla Qualità e Continuità dei servizi
- *Penali* in caso di mancata osservanza



SLA e Sicurezza

Ma sono anche in pratica l'**unico modo** per il Cliente di imporre e controllare le misure di sicurezza necessarie:

- Descrizione dettagliata delle misure di sicurezza da implementare
- Descrizione dettagliata del reporting
- Misure da implementare in caso di incidenti di sicurezza

...



SLA



Il punto di vista di Fornitore e Cliente sugli SLA sono diversi:

- Per il Fornitore sono misure tecniche da implementare (efficacemente)
- Per il Cliente sono gli strumenti di controllo sui servizi offerti dal Fornitore per:
 - Raggiungere gli obiettivi di Business
 - Implementare le Politiche di sicurezza



SLA Fornitore



- Descrizione tecnica del servizio (a basso livello)
- Caratteristiche garantite
- Descrizione dei metodi di misura
- Reporting
- Penali ecc.



SLA Cliente



A due livelli:

- Descrizione del servizio dal punto di vista del business:
 - Obiettivi di business
 - Garanzie, penali ecc.
- Descrizione dei singoli processi che lo compongono
 - Caratteristiche tecniche
 - Garanzie, metodi di misura, penali ecc.



SLA

- Gli SLA sono **critici** per il successo di un contratto di Outsourcing
- In pratica sono il vero strumento di controllo del contratto
- Devono essere rivisti periodicamente e frequentemente
- Devono essere elaborati insieme da Cliente e Fornitore per poter soddisfare le esigenze di entrambi



Grazie per l'attenzione