

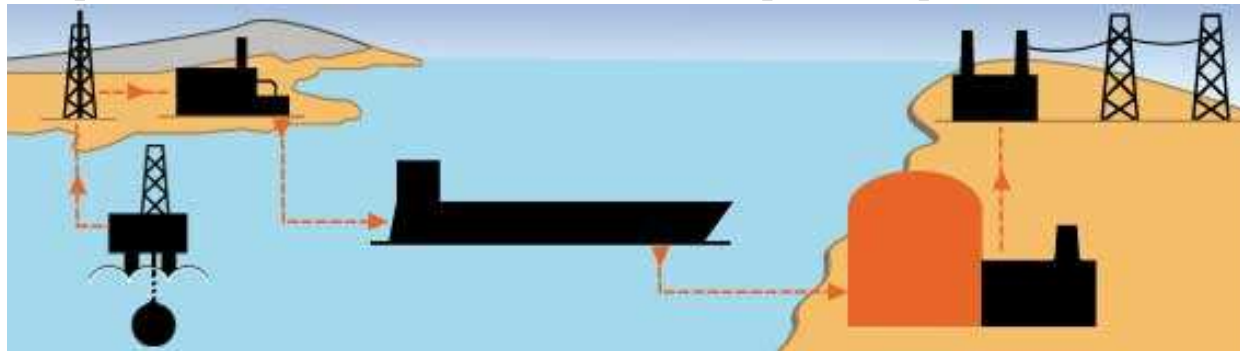
BS ISO/IEC 27001: 2005 per condensare la nuvola

Come si trattano i gas?

- Rendendoli liquidi
- Comprimendoli e inserendoli in contenitori

CONDENSANDOLI

... allora possono essere trattati, studiati, trasportati quindi sfruttati al meglio



Il CLOUD è lo “**stato gassoso**” dei dati ... intangibili apparentemente e quindi difficilmente controllabili

Come si condensa il nostro cloud

Bisogna riuscire a far tornare tangibili i dati ed i relativi trattamenti ed in questo la ISO 27001 può aiutare perché adottarla significa:

- Prendere coscienza dell'importanza dell'*asset* (*il nostro patrimonio informativo*)
- Darci delle regole e generare una "miglior pratica"
- Programmare e pianificare attentamente un *Statement of applicability* (SoA) e un *risk assessment* (*da cui può emergere l'evidenza di esternalizzare alcuni rischi*)
- Pianificare un buon funzionigramma (*... le dimensioni non contano*)
- Definire il perimetro entro il quale i dati si muovono e vengono trattati (*responsabili esterni al trattamento compresi*)

In una parola ?

CONSAPEVOLEZZA!

L'alternativa è scegliere quale delle tre vogliamo essere



Cosa implica avere consapevolezza del ISMS

Prendere consapevolezza del valore del nostro *asset* significa garantire sempre:

- *Confidentiality*
- *Integrity*
- *Availability* ... dei dati di cui siamo titolari

In alternativa l'*asset* perde valore (conseguenza di fatto) e probabilmente stiamo violando anche il codice della privacy!

Il vantaggio di un sistema di gestione della sicurezza efficace ed efficiente può essere anche quello di fornire maggiori garanzie di *compliance* normativa nostra e per i nostri partner

(non solo privacy ma anche d.lgs.231/01 per esempio)... **norma e funzionalità devono amalgamarsi – PAS 99**



Cosa significa il “bollino ISO 27001”? 1/2



Due cose prima di tutto:

1. Uscire dall'autoreferenzialità ed aver affrontato un iter di certificazione (133 control objectives and controls)
2. Il management dell'organizzazione ha la piena **consapevolezza** del valore dell'*asset* e se l'attività caratteristica è la gestione di dati di terzi può accadere che, anche se da punti di vista differenti, l'*asset* del cliente e del fornitore coincidano

In prima istanza:

Aspetti positivi: la sua sicurezza è la mia sicurezza

Aspetti negativi: possono nascere dei conflitti normativi o procedurali

Cosa significa il “bollino ISO 27001”? 2/2

Nel cloud la certificazione ISO 27001 è un valore aggiunto al servizio perché l'obiettivo dello standard è *"provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System"*.

Che sono parole che tutti noi vorremo riferite alla sicurezza del nostro patrimonio informativo ma....

Bisogna aggiungere che *"The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization"*

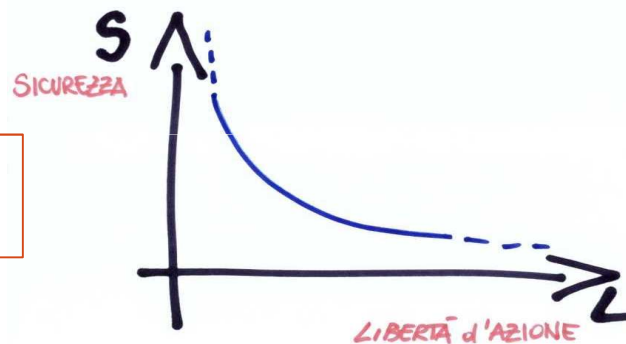
e questo non coincide sempre tra *hosting provider* e cliente.

Troppa sicurezza può essere negativa

Quindi affidarsi ad un Host ISO 27001 non equivale ad “affittare” un ISMS sicuro per noi ma per il fornitore. E’ sicuramente una buona garanzia ma è un aspetto da considerare quando si sceglie il servizio di *host*.

Avere un alto livello di sicurezza per esempio può appesantire la libertà d’azione

$$L = 1/S$$



*es: tempi di ripristino lunghi
ma con buon risultato in
termini di sicurezza ed
integrità dei dati*

In linea generale, comunque, chi eroga servizi web e si certifica pianifica l’intervento a favore della propria sicurezza cercandola di riflettere il più possibile su tutti gli *stakeholder*: è un vero e proprio investimento e come tale deve avere un ritorno e creare valore aggiunto

Cosa significa scegliere un provider ISO 27001”?

Ed il valore aggiunto può essere:

1. Business continuity (*BS 25999, BCM*)
2. Un ISMS aggiornato al fine di assicurarne l' idoneità, l' adeguatezza e l' efficienza
3. Audit di terza parte
4. Immagine di maggiore affidabilità
5. Maggiore trasparenza e centralità del cliente (retaggio del sistema PDCA della ISO 9001)
6. Parte del nostro ISMS certificato (?)
7. Vediamo direttamente un esempio [AMAZON](#)



Alcuni controlli della norma che possono interessare gli hosting provider

In riferimento ad utilizzo di servizi esternalizzati (all in one): I “subfornitori” devono essere sottoposti ad una attenta analisi e verifica dei requisiti (non solo tecnici)

A.5.2 External parties		
<i>Objective:</i> To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.		
A.5.2.1	Identification of risks related to external parties	<i>Control</i> The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.5.2.2	Addressing security when dealing with customers	<i>Control</i> All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A.5.2.3	Addressing security in third party agreements	<i>Control</i> Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

I rischi per le informazioni dell'organizzazione e le informazioni provenienti da processi aziendali che coinvolgono soggetti esterni devono essere identificati e controlli appropriati implementati prima di concedere l'accesso

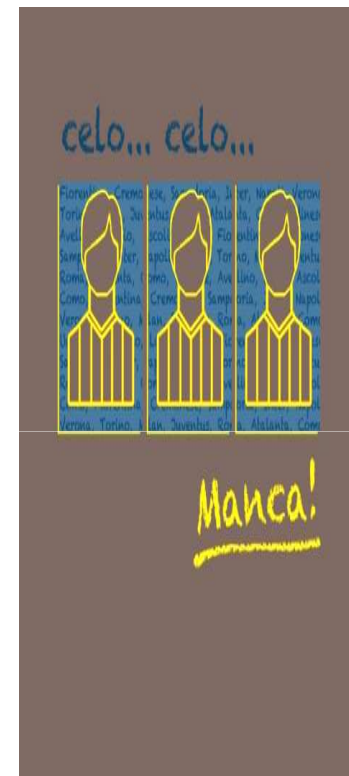
tutti i requisiti di sicurezza individuati devono essere affrontati prima di dare ai clienti l'accesso alle informazioni dell'organizzazione o delle attività

accordi con terzi che coinvolgono l'accesso, l'elaborazione, la comunicazione o la gestione delle informazioni dell'organizzazione o “facilities” (servizi, attrezzature) di trattamento delle informazioni, o l'aggiunta di prodotti o servizi per il trattamento delle informazioni devono rispettare tutti i requisiti di sicurezza pertinenti (valutazione secondo analisi dei rischi)

Alcuni controlli della norma che possono interessare il mondo cloud

ed ancora...

- Confidentiality agreements (A.6.1.5)
- Security of equipment off-premises (A.9.2.5)
- Secure disposal or re-use of equipment (A.9.2.6)
- Remove of property (A.9.2.7)
- Monitoring and review of third party services (A.10.2.2)
- Exchanges agreements (A.10.8.1/2/3)
- Managing changes to third party services (A.10.2.3)
- Outsourced software development (A.12.5.5)
- Business continuity and risk assessment(A. 14.1.2/3/4/5)
- Identification of applicable legislation (A.15.1.1)
- Data protection and privacy of personal information (A.15.1.4)



Alcuni controlli della norma che possono interessare gli hosting provider

Non dimentichiamo che dall'altra parte ci sono **sempre e comunque delle persone.**

La ISO 27001 pone un **forte accento** sul controllo del rapporto lavorativo tra organizzazione e risorsa umana (interna o esterna) distinguendo in controlli:



- Prima dell'assunzione (valutazione dei requisiti)
- Durante l'assunzione (sistema sanzionatorio, aggiornamenti...)
- Terminata l'assunzione (rimozione degli accessi/ clausole di riservatezza su contratti / controllo di fughe di know how aziendali – o di clienti)
- In caso di cambiamenti in organigramma (come per fine rapporto di lavoro)

In conclusione

Se un'organizzazione espone il bollino ISO 27001 ci sta dicendo:

- che, senza alcun dubbio, alcune procedure devono essere state adottate
- che i rischi, come combinazione di minacce e vulnerabilità sui processi certificati, sono stati attentamente analizzati in rapporto al valore dell'asset ($P_m * P_v * V_a = R_l$)
- che un ente terzo, indipendente e a sua volta certificato, ne verifica la conformità annualmente
- che in quell'azienda la idonea consapevolezza è stata raggiunta e le misure di sicurezza sono state conseguentemente adottate
- che, se le affidiamo i nostri dati, questi entreranno in un sistema con un alto standard di sicurezza
- che se anche noi vogliamo certificarci Iso 27001 possiamo trovare un sistema complementare (dove finisce uno inizia l'altro)

ARRIVEDERCI e GRAZIE

Andrea Orsi

Contatti:

- info@adivision.it
- www.adivision.it

www.adivision.it



Amadir
Alumni Master Diritto della Rete
www.amadir.it



openstudio
www.openstudioweb.it