Modello vettoriale per i Sistemi di Sicurezza delle Informazioni

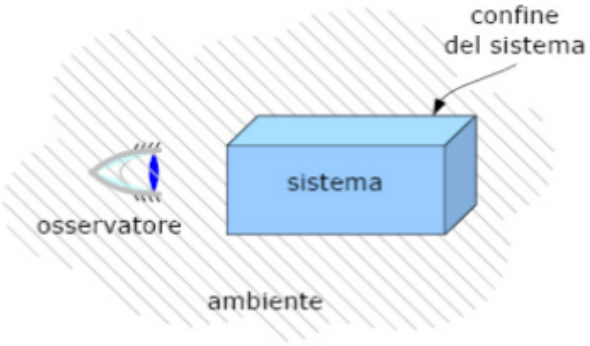
Author : Stefano Gorla

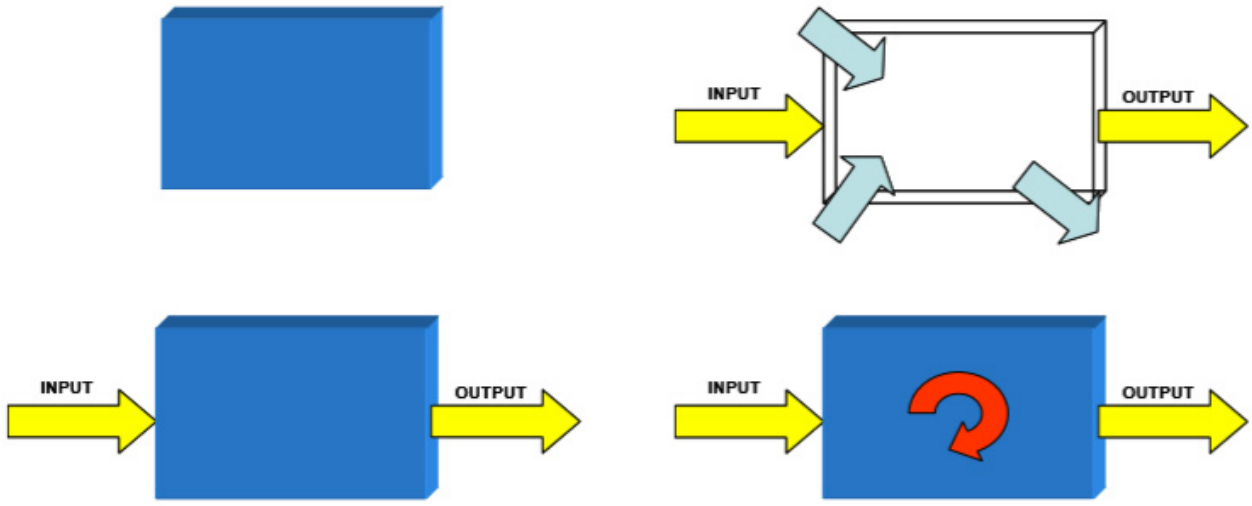
Date : 21 Gennaio 2019

La sicurezza dei dati e delle informazioni, è un asset fondamentale e strategico per le organizzazioni. I dati, e la loro gestione, sono la parte più importante e più critica delle organizzazioni.

All’interno delle organizzazioni, intese come sistema, i flussi dei dati, la loro conoscenza e gestione permettono di essere non solo competitivi ma proattivi nel campo della cybersecurity.

Un sistema è un insieme di attività e dati, a seguito di input, che reagisce a tali stimoli e si adatta per produrre output dedicati.



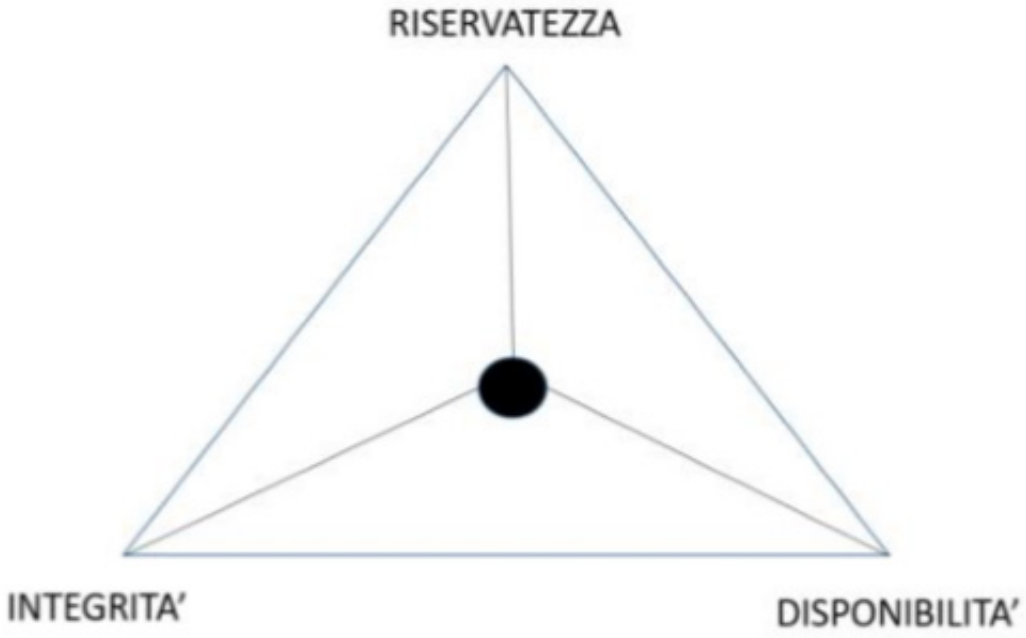


La sicurezza non è un prodotto ma un processo che si basa su aspetti organizzativi e tecnici.

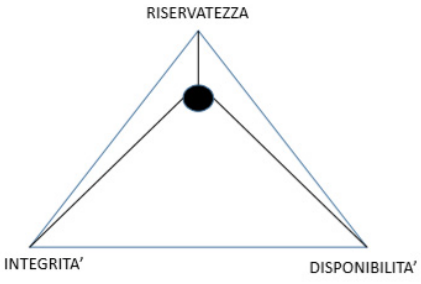
La sicurezza dei dati si basa su tre punti fondamentali:

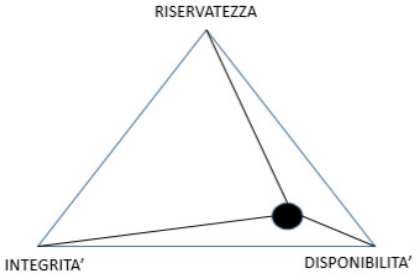
- Riservatezza
- Integrità
- Disponibilità

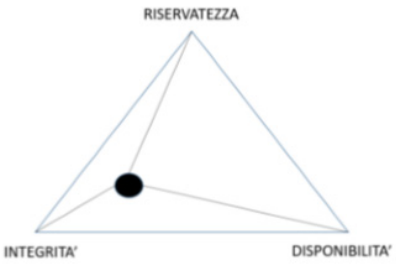
Questi punti sono i vertici di un triangolo equilatero. Al centro del triangolo, all'intersezione tra le mediane compare la posizione dell'organizzazione. Questa posizione deve essere bilanciata tra i tre vertici, uno spostamento verso un vertice comporta una diminuzione delle caratteristiche di un altro.



Ad esempio se sbilanciamo la struttura verso la disponibilità, attraverso vari storage o piani di DS (diffusione eccessiva), andiamo a compromettete la riservatezza dei dati.







Per analizzare lo stato dell'organizzazione rispetto a questi tre assi si è introdotto il concetto di vettore.

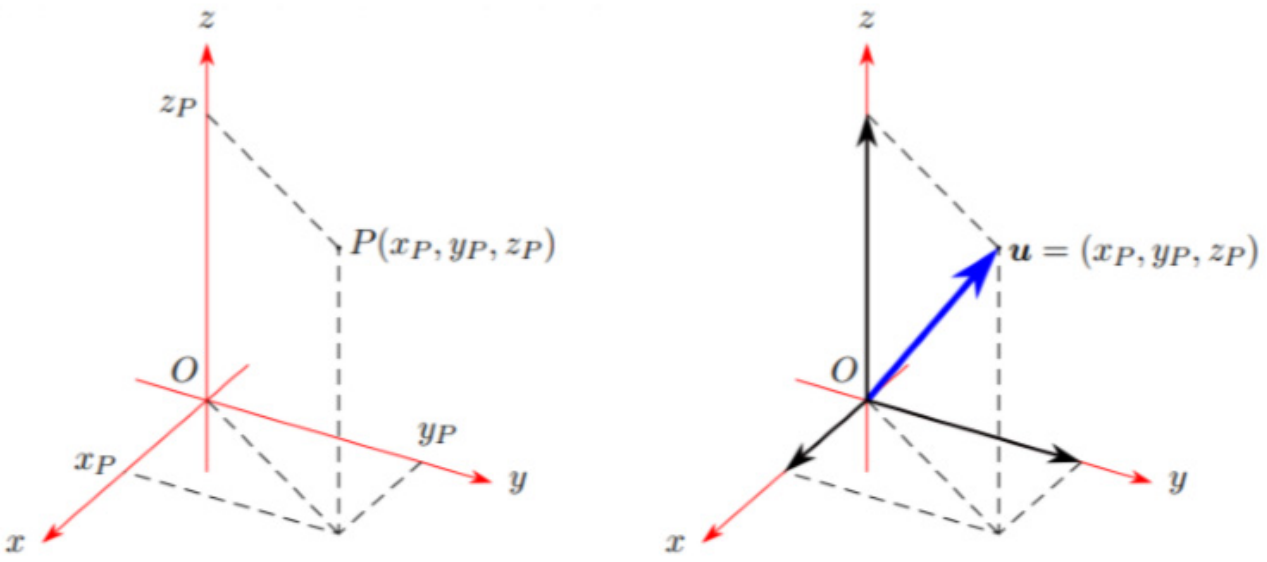
Un vettore è uno strumento matematico, largamente utilizzato in fisica, che possiede una direzione, un verso ed un'intensità e appartiene ad uno spazio vettoriale. Si descrive attraverso un formalismo

v=(vx, vy, vz)

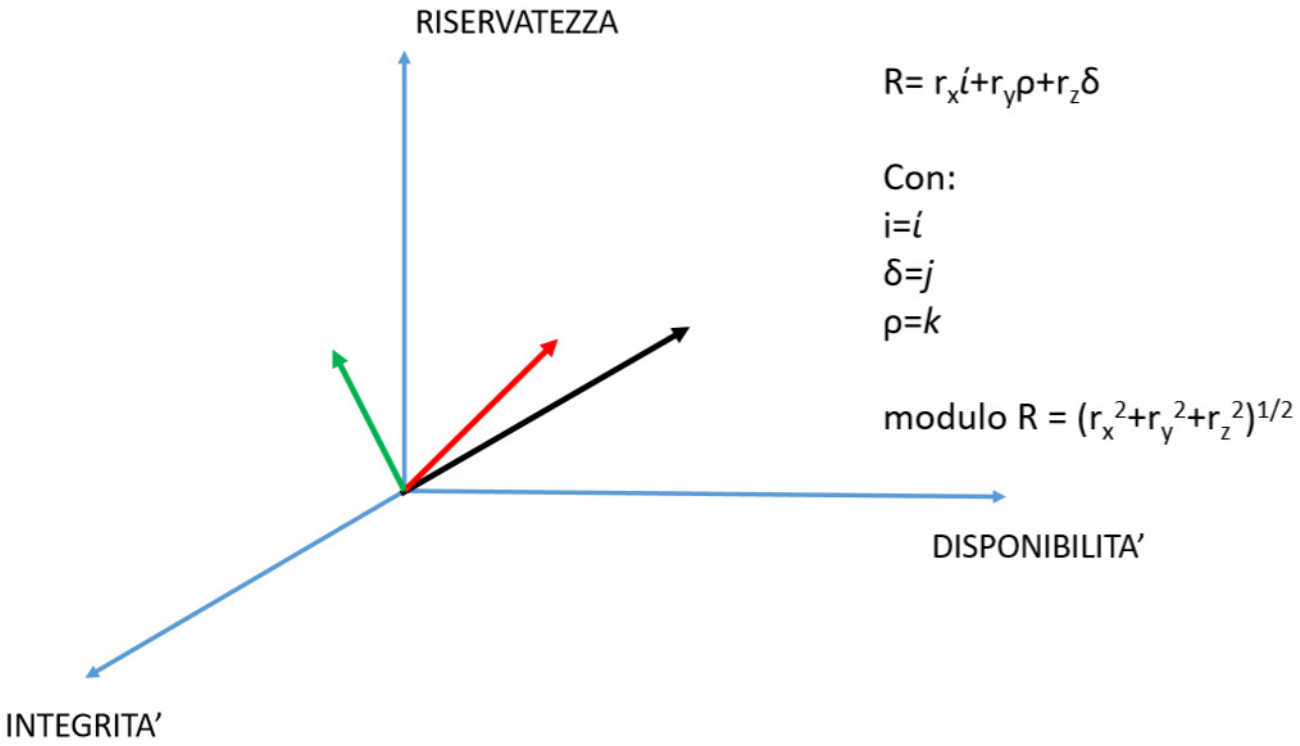
ovvero come combinazione lineare dei versori canonici

v=(vxi+vyj+vzk)

La posizione del punto sopra descritto è funzione quindi di tre coordinate: x, y, z.



Se andiamo a sostituire le coordinate canoniche con quelle relative allo spazio di Riservatezza, Integrità e Disponibilità, otteniamo un vettore funzione di queste.



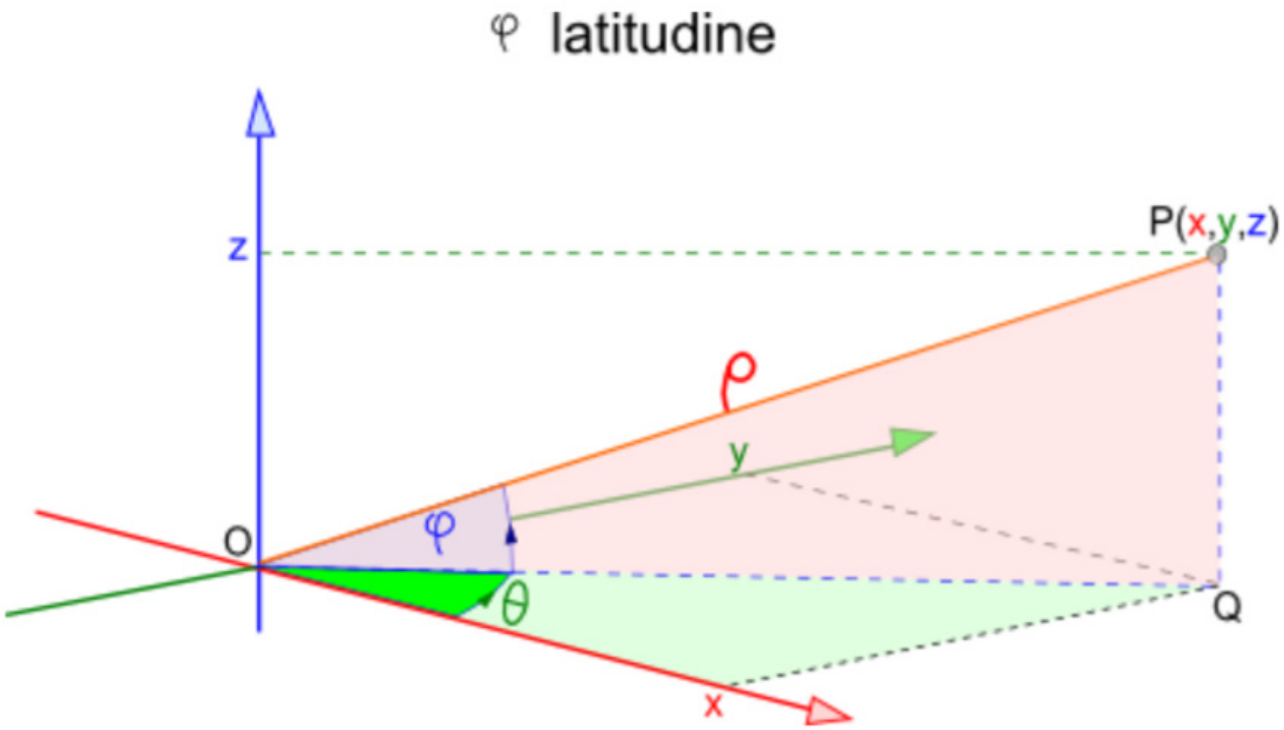
$R = r_x i + r_y \rho + r_z \delta$

Con:
$i = i$
$\delta = j$
$\rho = k$

modulo $R = (r_x^2 + r_y^2 + r_z^2)^{1/2}$

Altro parametro importante è il modulo del vettore dato dalla radice quadrata della somma dei quadrati delle singole proiezioni sugli assi.

Non ultimo, in questo spazio, è bene introdurre il concetto di latitudine, ovvero la posizione del punto relativa a due angoli formati tra le proiezioni dei vettori.



Si è indicata una scala di riferimento che possa descrivere lo stato di applicazione del sistema. In particolare si è utilizzata la seguente scala:

0 = Non Applicato

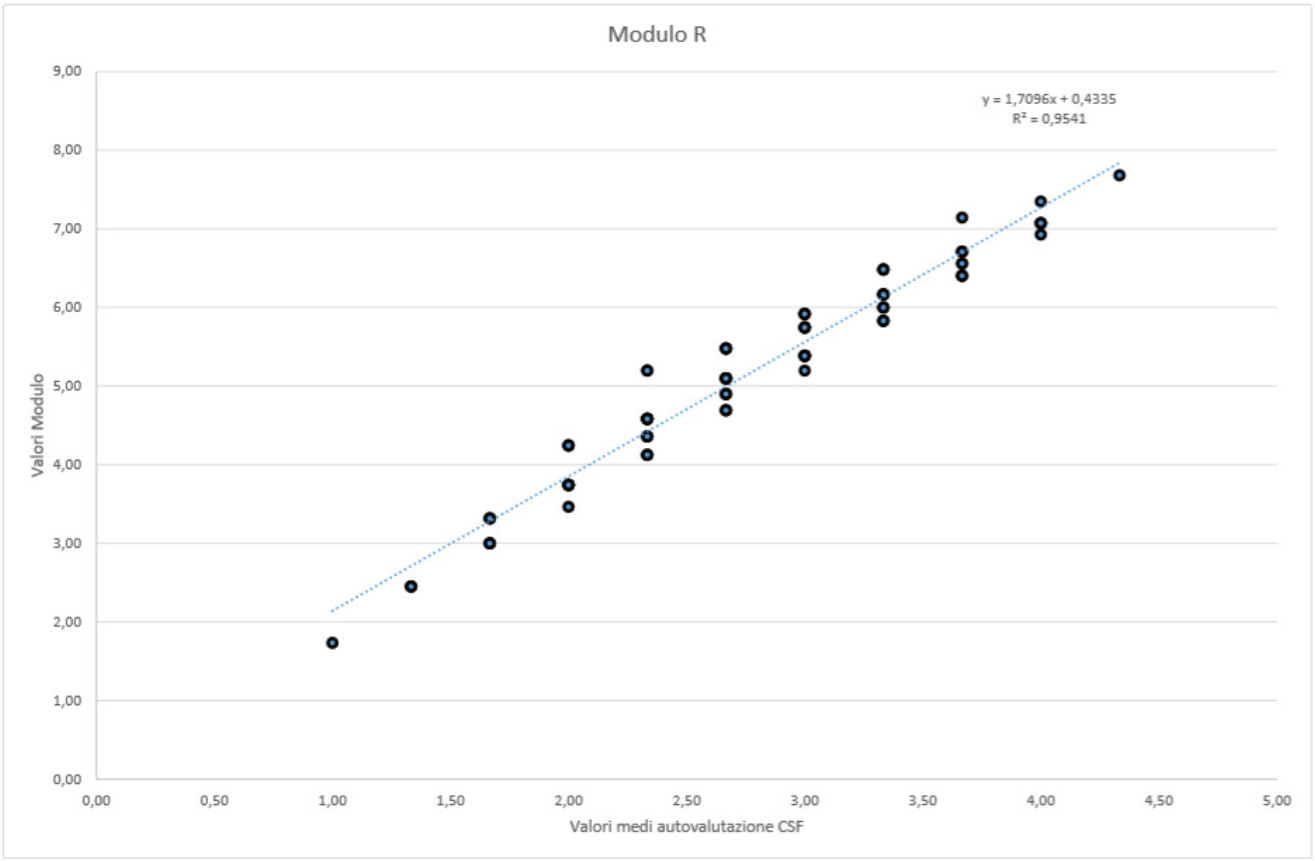
1 = Parzialmente implementato, non completamente definito né convalidato

2 = parzialmente implementato, completamente definito e accettato

3 = pienamente o molto ampiamente implementato, definitivo ("statico")

4 = implementato dinamicamente, controllato e migliorato permanentemente

A questo punto si sono graficati i valori dei moduli e degli angoli come illustrato nelle immagini seguenti.


Modulo R
y = 1,7096x + 0,4335
R² = 0,9541
Valori Modulo
Valori medi autovalutazione CSF
9,00
8,00
7,00
6,00
5,00
4,00
3,00
2,00
1,00
0,00
0,00
0,50
1,00
1,50
2,00
2,50
3,00
3,50
4,00
4,50
5,00

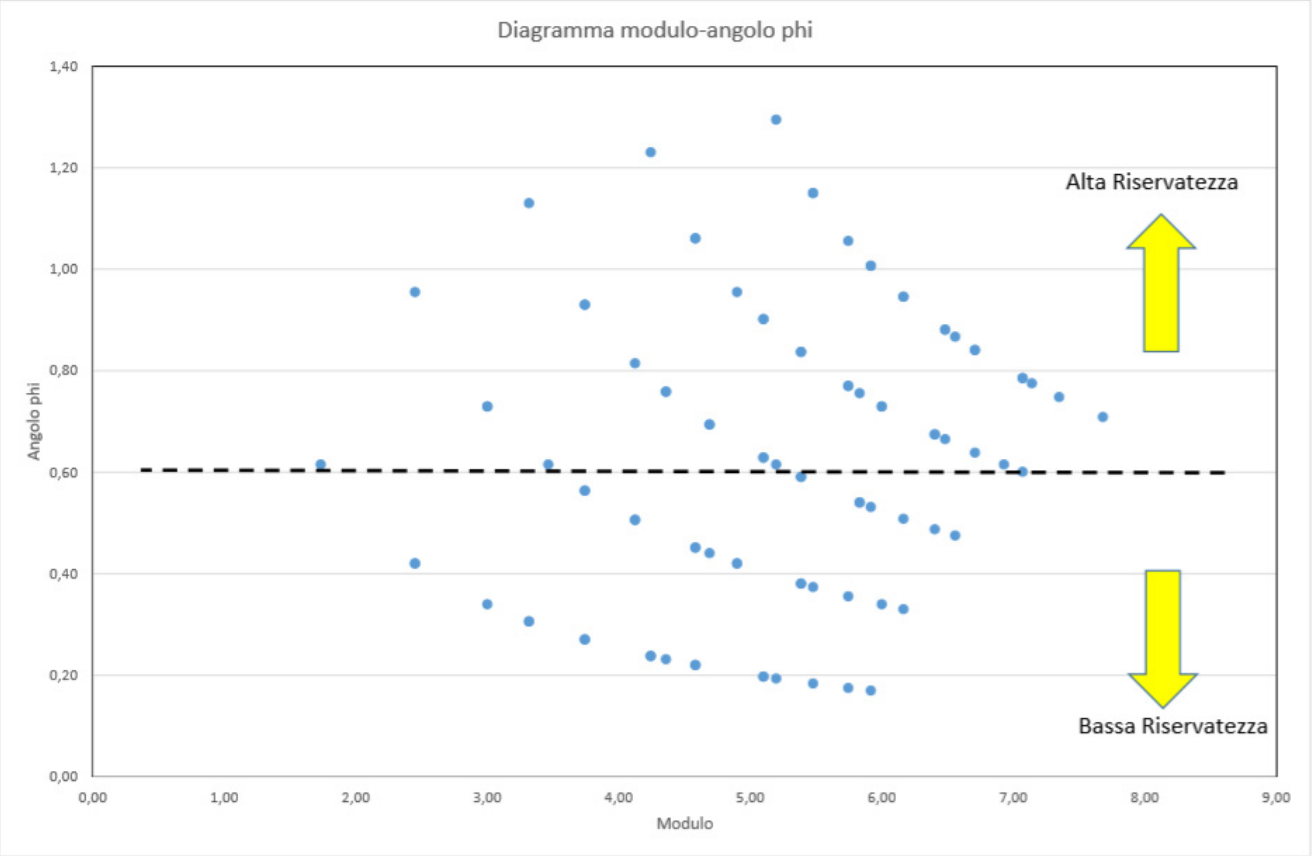
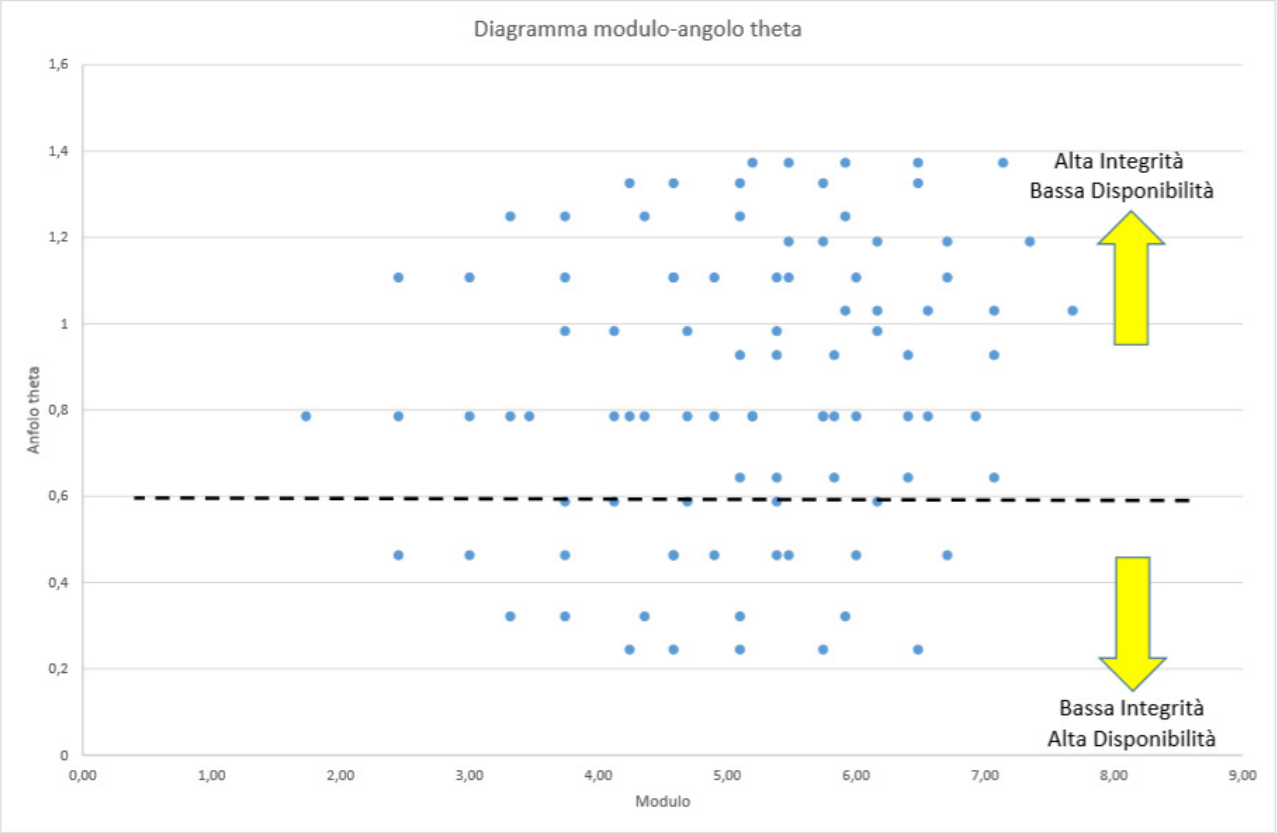


Diagramma modulo-angolo phi
Angolo phi
Modulo
1,40
1,20
1,00
0,80
0,60
0,40
0,20
0,00
0,00
1,00
2,00
3,00
4,00
5,00
6,00
7,00
8,00
9,00
Alta Riservatezza
Bassa Riservatezza



Si è utilizzato il CSF NIST, Cyber Security Framework NIST, per una autovalutazione dello stato del sistema organizzazione

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

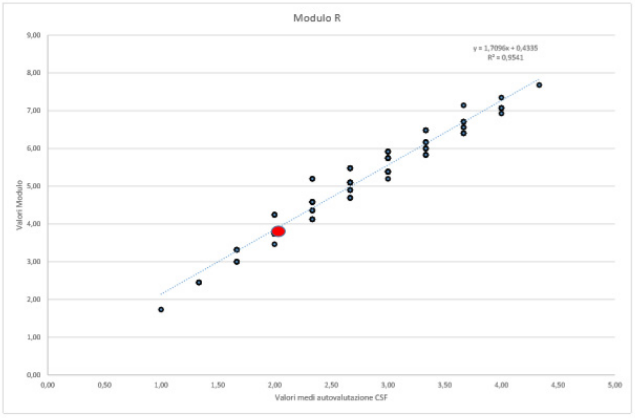
Per ogni domanda del framework sì è attribuito un valore all’applicazione del sistema riferito agli assi Riservatezza, integrità e Disponibilità.

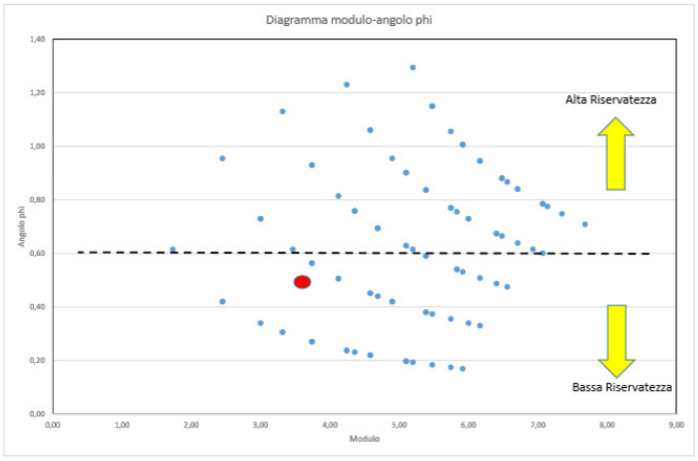
Un esempio è riportato sotto.

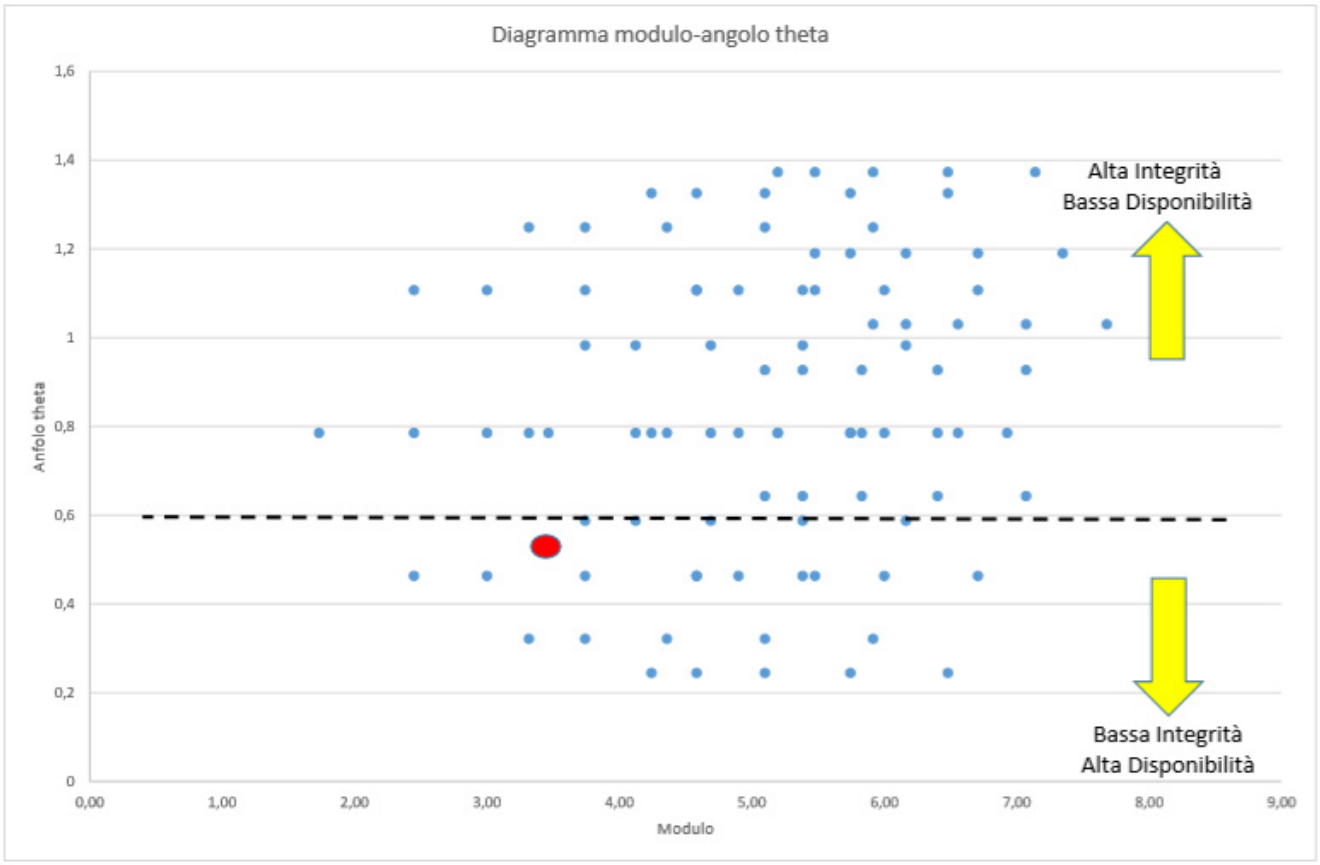
	IDENTIFY	NIST CORE FRAMEWORK	I	R	D
Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM1	Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	4		
	ID.AM2	Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	4		
	ID.AM3	I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	4	4	4
	ID.AM4	I sistemi informativi esterni all'organizzazione sono catalogati	3	3	3
	ID.AM5	Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	3	3	3
	ID.AM6	Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)		3	

Per ogni asse viene poi eseguita la media dei valori così ottenuti, in modo da identificare lo stato aziendale.

Riportando sui grafici illustrati sopra i valori ottenuti, si ha immediatamente un’immagine di come è posizionata l’organizzazione in funzione dei tre parametri e come questi sono bilanciati.







Dall'analisi dei grafici emerge immediatamente quali parametri sono da implementare o diminuire per avere un perfetto bilanciamento tra di essi. E' poi una scelta organizzativa quella di mantenere tale bilanciamento/sbilanciamento o implementare i piani d'azione necessari.

Questo processo può essere iterato e diffuso a cascata anche all'interno dell'organizzazione, ad esempio per businness unit o reparto, riportando i valori ottenuti per ogni unità organizzativa permette una visione di dettaglio che può essere aggregata per fornire informazioni generali

sull’organizzazione.

Conclusioni

Si è cercato di realizzare un modello di analisi vettoriale per verificare lo stato in un sistema di gestione della sicurezza dei dati e delle informazioni. Attraverso una autovalutazione, utilizzando un framework di riferimento internazionale, e del grado di copertura di implementazione dell’item, si è potuto ottenere una fotografia del posizionamento dell’organizzazione e dell’eventuale sbilanciamento relativamente ai parametri Riservatezza, integrità e Disponibilità.

Articolo a cura di **Stefano Gorla**