Performance dei sistemi di gestione per la sicurezza delle informazioni

Author : Anastasia Ambesi

Date : 14 novembre 2018

La valutazione delle performance di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è il cuore centrale della fase di Check del noto ciclo PDCA sotteso al SGSI stesso e trova le sue fondamenta nella corretta progettazione del SGSI. Nel seguito viene illustrata la catena logica che porta all'individuazione dell'insieme di attività richieste per il controllo delle performance di un SGSI, comprendendo anche la definizione di alcune metriche di valutazione delle performance del SGSI, partendo dalla sua definizione.

Ogni sistema di gestione per la sicurezza delle informazioni è costituito da un insieme di risorse composto da persone, responsabilità, informazioni e procedure impiegate da un'organizzazione per raggiungere e mantenere gli obiettivi di sicurezza delle informazioni definiti in termini di riservatezza, integrità e disponibilità.

Dal momento che l'informazione è di per sé un asset aziendale, ovvero un bene che aggiunge valore all'organizzazione e considerando che la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri asset informativi, e non solo, in un contesto dove i rischi informatici sono in continuo aumento. La norma ISO/IEC27001[1], come noto, definisce i requisiti per impostare, gestire e mantenere un SGSI, in modo trasversale rispetto il mercato, e richiama aspetti relativi alla sicurezza logica, fisica ed organizzativa.

La sicurezza delle informazioni comporta l'applicazione e la gestione di misure di sicurezza adeguate e proporzionate al contesto di riferimento, che possono implicare la considerazione di una vasta gamma di minacce, con l'obiettivo di garantire il raggiungimento e mantenimento nel tempo degli obiettivi di business e di sicurezza, anche in situazioni avverse, riducendo al minimo l'impatto di eventuali incidenti relativi alla sicurezza delle informazioni.

Tale obiettivo di sicurezza è ottenuto attraverso l'implementazione di una serie di controlli di sicurezza, selezionati per mitigare i rischi evidenziati durante il risk assessment.

Questi controlli devono essere specificati, attuati, monitorati, riesaminati e migliorati, per assicurare che gli specifici obiettivi di sicurezza delle informazioni e di business siano raggiunti. I pertinenti controlli relativi alla sicurezza delle informazioni dovrebbero, quindi, essere perfettamente integrati con i processi di business di un'organizzazione.

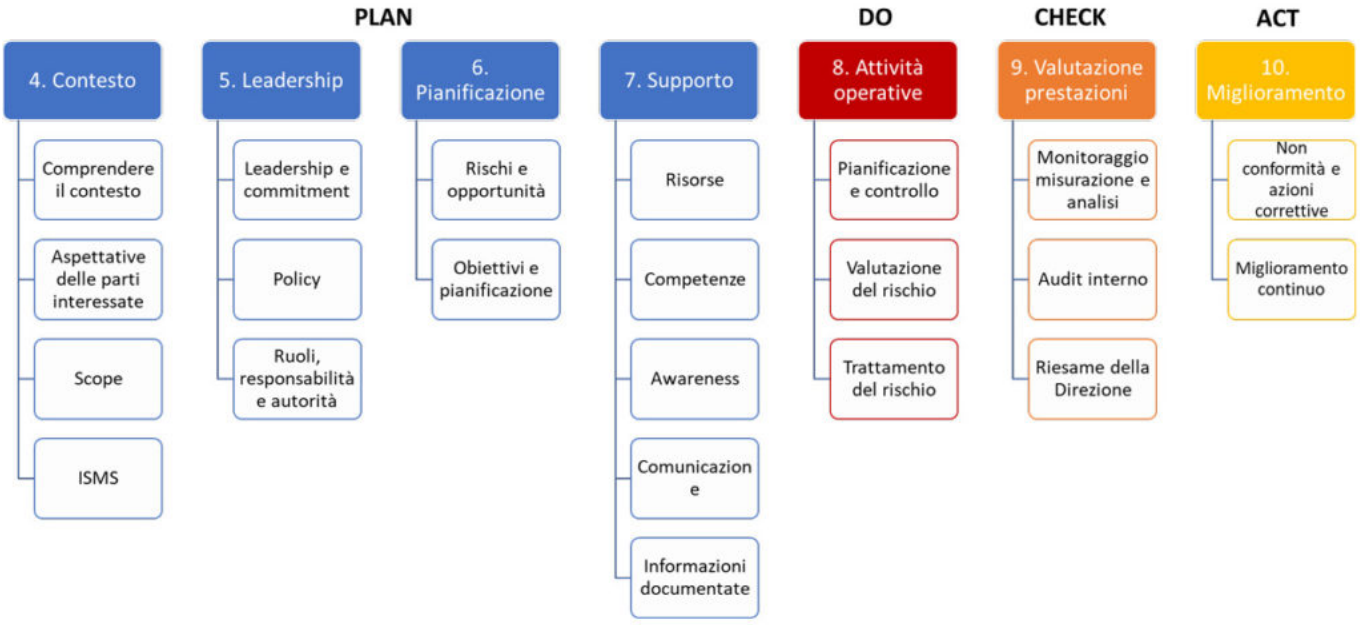
Anche la norma ISO/IEC 27001 è mappabile sul modello di Deming, così come avviene per altre norme (ad esempio la ISO 9001). Questo modello, indicato notoriamente con l'acronimo PDCA, si suddivide in quattro fasi ciclicamente e continuamente ripetute: Plan (pianificare), Do (eseguire), Check (controllare), Act (agire).

Nella fase di **Plan**, si definisce lo scopo del SGSI e le politiche che lo guidano, sono identificati gli obiettivi ed i mezzi per raggiungerli, è stabilito il processo di analisi del rischio, sono individuate le risorse necessarie.

La fase **Do** si preoccupa di realizzare il programma che è stato pianificato, viene eseguito il risk assessment e tutti i controlli e le procedure che sono state previste, vengono implementate.

Nella fase di **Check**, si valutano le performance del SGSI.

La fase **Act** prevede di intraprendere azioni correttive per indirizzare eventuali non conformità e nell'ottica del miglioramento continuo, migliorare la sostenibilità, l'adeguatezza, l'efficacia del SGSI.



Al fine di valutare la performance del SGSI, occorre approfondire le fasi *Check* e *Act* del suddetto Ciclo di Deming.

Relativamente al monitoraggio delle prestazioni e dell'efficacia del SGSI, l'organizzazione

deve innanzitutto determinare:

- cosa è necessario monitorare e misurare, includendo i processi e i controlli relativi alla sicurezza delle informazioni;
- i metodi per il monitoraggio, la misurazione, l'analisi e la valutazione, per quanto applicabile, per assicurare risultati validi;
- quando il monitoraggio e la misurazione devono essere effettuati;
- chi deve monitorare e misurare;
- quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati;
- chi deve analizzare e valutare questi risultati.

Per fare ciò, lo strumento più indicato è costituito da indicatori di performance (Key Performance Indicators -KPI), che permettono di valutare le prestazioni di un determinato target.

Un KPI costituisce un indicatore quantitativo dell'efficacia ed efficienza di un controllo di sicurezza tecnologico, procedurale e/o organizzativo, in relazione agli obiettivi di sicurezza definiti ed al relativo piano per il loro raggiungimento.

Idealmente è possibile considerare un KPI come una variabile controllata in uscita ad un sistema di controllo, il cui valore è quindi determinabile a partire da un certo numero di variabili in ingresso, che coincidono con l'implementazione pratica di misure/verifiche a sostegno dei piani di sicurezza.

Per ***variabile controllata*** si intende un indicatore quantitativo sintetico che esprime lo stato di un particolare elemento di un processo di business dal punto di vista della sicurezza.

Le ***variabili di controllo*** sono, invece, elementi su cui è possibile agire per modificare nel tempo il valore della variabile controllata. Identificano le aree di intervento possibili nel particolare ambito rappresentato dalla variabile controllata.

La scelta degli indicatori più utili dipende da diversi elementi e può essere guidata da tre dimensioni: **ambito**, **oggetto** ed **esigenza** di misurazione [2].

Nella tabella seguente viene riportato qualche esempio di KPI in ambito di implementazione ISO/IEC 27001:

INDICATORE	**MODALITA' DI CALCOLO**	**CAMPIONAMENTO**
Etichettatura informazioni	Num. informazioni etichettate/num. informazioni etichettabili	Annuale
Dismissione dei supporti	Num. supporti dismessi/num. supporti non più necessari	Annuale
Anti-malware non aggiornati	Num. antivirus obsoleti/num. totale di	Settimanale

	workstation con antivirus aggiornato	
Disponibilità del servizio	Disponibilità totale/Massima disponibilità esclusi i tempi di inattività	Mensile/Annuale
Sistemi informativi critici	Num. sistemi informativi critici/Num. sistemi informativi	Semestrale
Livello di vulnerabilità	Num. vulnerabilità per Severity/Sistemi a perimetro	Mensile
Information Security Incident	Numero di IS incident (pre introduzione SGSI)/numero di IS incident (post introduzione SGSI)	Annuale
Rapporti con i fornitori	Assessment condotti sui servizi erogati /Num. di servizi erogati	Annuale

Figura 2: esempi di indicatori

L’obiettivo principale per lo sviluppo e l’implementazione di processi di misurazione di un SGSI risiede nella creazione di una base informativa che consenta all’organizzazione di acquisire, analizzare e comunicare informazioni relative ai processi definiti nell’ambito del proprio SGSI.

Questi dati, adeguatamente raccolti ed organizzati, forniranno informazioni sullo stato del SGSI, e andranno utilizzati per adottare decisioni inerenti al suo sviluppo ed al miglioramento dell’implementazione.

In questo ambito assume un utile rilievo la norma ISO/IEC 27004 “Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation”[3] la quale aiuta a valutare le prestazioni di sicurezza delle informazioni e l'efficacia di un sistema di gestione per la sicurezza delle informazioni al fine di soddisfare il requisito 9.1 della ISO/IEC 27001: monitoraggio, misurazione, analisi e valutazione.

I risultati del monitoraggio e della misurazione di un SGSI possono essere di supporto alle decisioni relative alla governance, alla gestione, all'efficacia operativa e al miglioramento continuo del SGSI stesso.

L’organizzazione deve conservare appropriate informazioni documentate quale evidenza dei risultati dei monitoraggi e delle misurazioni effettuate.

Per valutare se il proprio SGSI sia conforme ai requisiti richiesti dallo standard internazionale e sia efficacemente attuato e mantenuto, viene utilizzato lo strumento dell’***audit interno***.

A tal fine, l’organizzazione:

- pianifica uno o più programmi di audit;
- definisce i criteri di audit e il campo di applicazione;
- seleziona gli auditor e conduce gli audit in modo da assicurare l'obiettività e l'imparzialità del processo di audit;
- assicura che i risultati degli audit siano riportati ai relativi responsabili;
- conserva informazioni documentate quale evidenza dell'attuazione del programma di audit e dei risultati.

I principali vantaggi derivanti da monitoraggio, misurazione, analisi e valutazione possono includere:

- **maggiore responsabilità**: vi è un aumento di responsabilità per la sicurezza delle informazioni, aiutando a identificare specifici processi o controlli che sono implementati in modo non corretto, non sono implementati o sono inefficaci;
- **miglioramento delle prestazioni di sicurezza delle informazioni e dei processi**: si consente alle organizzazioni di quantificare i miglioramenti nella protezione delle informazioni nell'ambito del loro SGSI e dimostrare progressi quantificabili nel raggiungimento dei propri obiettivi di sicurezza delle informazioni;
- **evidenze del rispetto dei requisiti**: è possibile fornire prove documentate che dimostrino il rispetto dei requisiti ISO/IEC 27001 (e di altri standard), quali leggi applicabili, norme e regolamenti;
- **supporto al processo decisionale**: può essere supportato un processo decisionale basato sul rischio, contribuendo con informazioni quantificabili al processo di gestione del rischio: si può consentire alle organizzazioni di misurare i successi e i fallimenti degli investimenti passati e attuali in materia di sicurezza delle informazioni e fornire dati quantificabili in grado di supportare l'allocazione delle risorse per gli investimenti futuri.

Al fine di assicurarne la continua idoneità, adeguatezza ed efficacia, l'alta Direzione, a intervalli pianificati, riesamina il SGSI implementato.

Il riesame della Direzione include considerazioni su:

- lo stato delle azioni derivanti dai precedenti riesami di direzione;
- i cambiamenti dei fattori esterni e interni che hanno attinenza col SGSI;
- le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, compresi gli andamenti:
    - delle non conformità e azioni correttive;
    - dei risultati del monitoraggio e della misurazione;
    - dei risultati di audit;
    - del raggiungimento degli obiettivi per la sicurezza delle informazioni;
- le informazioni di ritorno dalle parti interessate;
- i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio;
- le opportunità per il miglioramento continuo.

Gli output derivanti dal riesame della Direzione comprendono, dunque, decisioni relative alle opportunità per il miglioramento continuo e ogni necessità di modifiche al SGSI.

In conclusione, la valutazione delle performance del SGSI è un processo che per sua natura deve essere integrato nei processi operativi aziendali al fine di fornire misurazioni utili a supportare la determinazione di decisioni aziendali. L'insieme di queste valutazioni può confluire in una sorta di cruscotto aziendale, di complessità variabile a seconda del contesto organizzativo, utilizzato dal Management per valutare costantemente e puntualmente il raggiungimento o meno degli obiettivi prefissati. Come ogni processo, anche la valutazione delle performance del SGSI deve essere **progettata**, **pianificata**, **attuata** e **misurata**, al fine di individuare eventuali scostamenti rispetto gli obiettivi che hanno portato alla sua determinazione. L'introduzione di strumenti software COTS, con set di KPI predeterminati, può rappresentare un valido supporto solo se permette di modellare in modo "sartoriale" le necessità di analisi e reporting dell'organizzazione, evitando quindi ogni elemento non in linea con gli obiettivi e le esigenze dell'organizzazione stessa.

BIBLIOGRAFIA

[1] ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements

[2] *Thomas Castagna - Luciano Quartarone*, Information Security Performance, https://www.ictsecuritymagazine.com/articoli/information-security-performance/

[3] ISO/IEC 27004 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation

Articolo a cura di **Anastasia Ambesi**