



CYBERSA

We make **cyber security**
simple for you

Secure Lean IT

Ing. Adolfo Di Fonzo CISM

4 Ottobre 2024



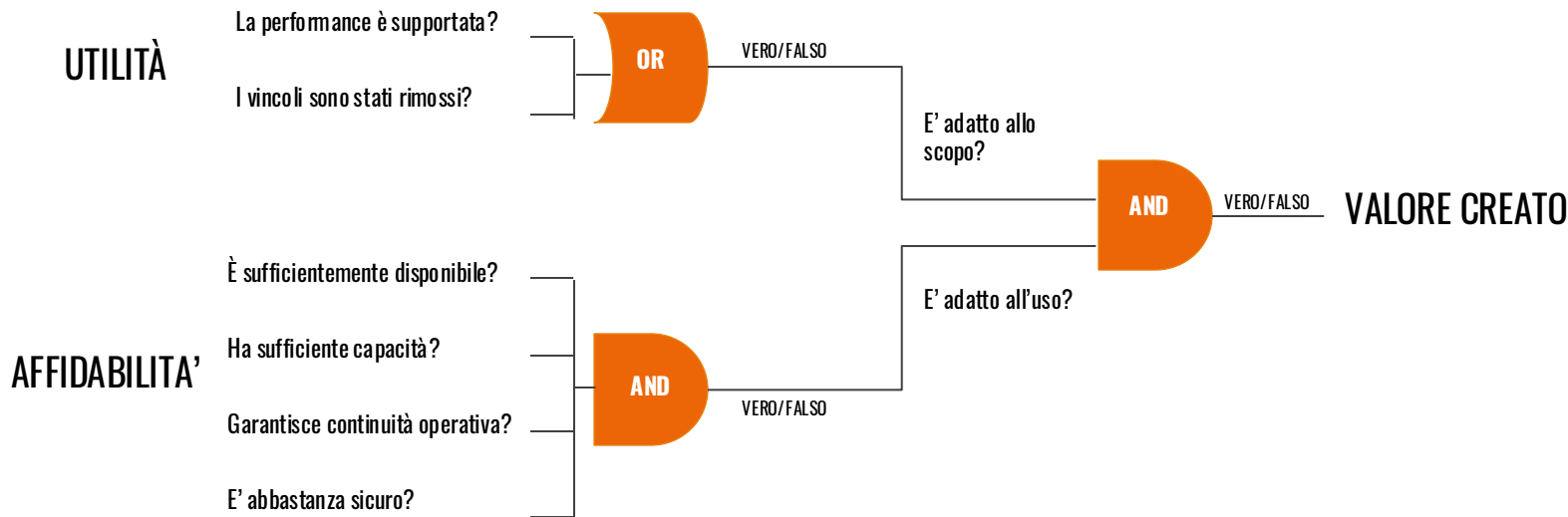
Innovazione e sicurezza

Come trovare il giusto
equilibrio: un approccio
metodologico

- < Lo sviluppo del business tra utilità e garanzia di affidabilità e sicurezza
- < Come trovare il giusto equilibrio e creare Valore
- < Buone Pratiche che aumentano l'affidabilità di un sistema

Innovazione e Sicurezza

Lo sviluppo del business tra utilità e garanzia di affidabilità e sicurezza



UTILITÀ + AFFIDABILITA' = VALORE



Come trovare il giusto equilibrio e creare Valore

Quali sono i fattori abilitanti che permettono ad un'organizzazione di raggiungere un equilibrio fra queste leve:



Design sicuro: ridurre le vulnerabilità di una web app includendo nella progettazione il threat modeling.



Utilizzo di tecnologie e strumenti di sicurezza avanzati: utilizzare sistemi di autenticazione multi fattore, crittografia dei dati e monitoraggio della sicurezza.



Formazione degli utenti: fornire agli utenti informazioni su come proteggere le proprie informazioni e come riconoscere e segnalare attività sospette.

A woman with curly hair, wearing a black, sleeveless, floor-length dress, is bent over at the waist, looking down. She is standing in a flat, open field. To her left is a tree with a thick, gnarled trunk that leans at a sharp angle towards the right. The tree's canopy is dense and rounded, with a dark, almost black color. The background is a clear sky with a gradient of colors from light blue at the bottom to a pale yellow and orange at the top, suggesting a sunset or sunrise. The word "Resilienza" is written in a black, serif font across the middle of the image, positioned to the left of the woman and below the tree's canopy.

Resilienza

Innovazione, Sicurezza e Resilienza

Buone Pratiche che aumentano l'affidabilità di un sistema



Security by Design

Un approccio proattivo per
l'innovazione

- < Integrazione della sicurezza fin dalle prime fasi di progettazione
- < Take Action!!
- < Agile e Lean: strumenti di trasformazione dei processi IT al servizio della Sicurezza

Security By Design

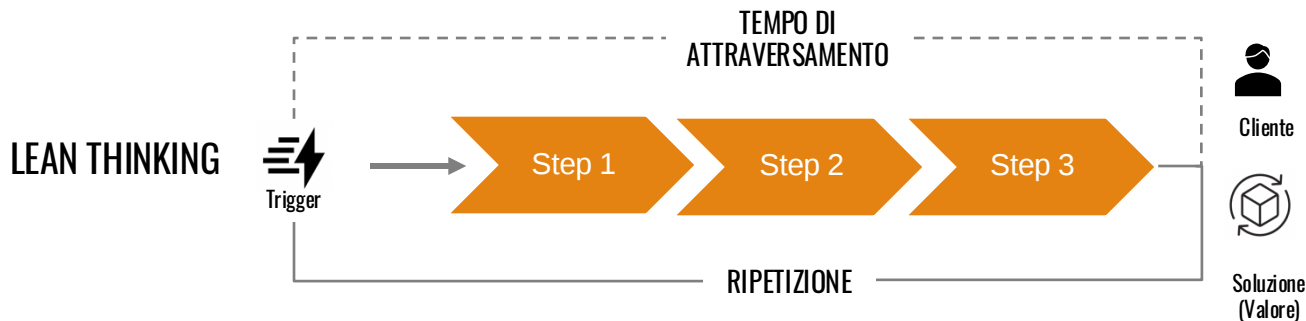
Integrazione della sicurezza fin dalle prime fasi di progettazione

I suoi principi fondamentali sono:

- ✓ Prevenzione anziché rimedio
- ✓ Sicurezza come impostazione predefinita (Security by Default)
- ✓ Sicurezza integrata nella progettazione
- ✓ Funzionalità completa senza compromessi
- ✓ Sicurezza end-to-end
- ✓ Visibilità e trasparenza
- ✓ Rispetto della sicurezza dell'utente

Security By Design

Take Action!!



PRINCIPI

- 1 Precisare esattamente il valore per prodotto
- 2 Identificare il flusso di valore per ogni prodotto
- 3 Far scorrere il valore senza interruzioni
- 4 Consentire al cliente di tirare il valore dal produttore
- 5 Perseguire la perfezione

"Adattamento della Sicurezza delle Informazioni nel Mondo Agile" del Journal ISACA - Gerald Pang

Come le organizzazioni possono adattare le loro strategie di sicurezza delle informazioni per adattarsi ai framework Agile, garantendo sia agilità che sicurezza nelle loro operazioni.

- **Agile e Sicurezza delle Informazioni:** esiste un potenziale conflitto tra le metodologie Agile e le pratiche di sicurezza delle informazioni. I team Agile spesso danno priorità alla funzionalità e al valore aziendale rispetto alla conformità alla sicurezza, mentre gli auditor IT e i professionisti della conformità preferiscono un approccio coerente e documentato.
- **Incorporare la Sicurezza in Agile:** uso dei 10 Principi Lean-Agile del SaFe per adattare gli approcci alla sicurezza IT. Importanza del pensiero sistemico, dove la sicurezza IT e la gestione del rischio sono parti integrali dell'intero sistema, inclusi design, sviluppo e operazioni.
- **Bilanciare Sicurezza e Agilità:** assumere variabilità e preservare opzioni, adottare una visione economica dei controlli di sicurezza, organizzarsi intorno al valore, costruire incrementalmente con cicli di apprendimento rapidi e decentrare il processo decisionale. L'obiettivo è integrare la sicurezza in modo che supporti l'ambiente Agile rapido e dinamico.
- **Sfide e Opportunità:** richiede un cambiamento di mentalità e approccio per allineare la sicurezza IT e la gestione del rischio con le metodologie Agile.

Principio Lean-Agile	Approcci Correlati alla Sicurezza
Applica il pensiero sistemico	Sicurezza all'interno del sistema
Presumi la variabilità e preserva le opzioni	Principi di sicurezza come faro per la variabilità
Adotta un punto di vista economico	Controlli di sicurezza con una visione economica
Punta al valore	Sicurezza gestita intorno al valore
Costruisci incrementalmente con cicli di team rapidi e integrati	Integrazione e automazione degli strumenti di sicurezza per supportare iterazioni rapide e incrementali
Visualizza e limita il lavoro in corso (WIP), riduci le dimensioni dei lotti e gestisci le lunghezze delle code	WIP limitato e riduzione delle dimensioni dei lotti per i controlli di sicurezza e le implementazioni
Applica la cadenza, sincronizza con la pianificazione trasversale	Applicazione della cadenza di sicurezza, sincronizzazione con la pianificazione trasversale
Basa le milestone su valutazioni obiettive dei sistemi di lavoro	Chiarimento dei requisiti e degli obiettivi di sicurezza per ogni milestone
Sblocca la motivazione intrinseca dei lavoratori sulla conoscenza	Sbloccare la motivazione intrinseca per la sicurezza
Decentralizza il processo decisionale	Potenziamento del team con conoscenza e autorità decisionale sulla sicurezza

SECURE Lean IT

Come integrare la Sicurezza nei
Processi

- < Incorporare la sicurezza nel processo di miglioramento continuo
- < Un modello per il miglioramento Continuo
- < SECURE nel processo di miglioramento continuo

Incorporare la sicurezza nel processo di miglioramento continuo - I

- Per incorporare efficacemente la sicurezza in un processo LEAN, è necessario adottare un approccio che aiuti ad **integrare in modo sistematico** e ripetitivo la **sicurezza** in ogni fase di un processo di **miglioramento continuo** del prodotto/servizio.
- Questo implica pensare proattivamente alla sicurezza quando si:
 - ✓ definiscono gli obiettivi
 - ✓ misurano i processi
 - ✓ analizzano i dati
 - ✓ implementano miglioramenti
 - ✓ controllano i risultati.
- Tale approccio vuole assicurare che la sicurezza non sia un “dopo ci penso”, ma una **componente** integrata e **fondamentale** del processo di miglioramento.

Incorporare la sicurezza nel processo di miglioramento continuo - II

- La sicurezza deve essere una priorità assoluta per l'organizzazione, in tutte le sue fasi e processi. Deve essere integrata in modo nativo nelle attività aziendali, piuttosto che essere considerata un'aggiunta secondaria. (**SECURITY EMBEDDED INTO DESIGN**)
- Le misure di sicurezza devono essere integrate nei processi aziendali senza comprometterne l'efficienza. Devono essere progettate e implementate in modo da essere compatibili con i processi esistenti e non costituire un ostacolo alla produttività. (**FULL FUNCTIONALITY**)
- Le pratiche di sicurezza devono essere migliorate costantemente per adattarsi alle mutevoli minacce e ai cambiamenti organizzativi. Devono essere periodicamente riviste e aggiornate, al fine di garantire che siano efficaci nel proteggere l'organizzazione. (**PROACTIVE NOT REACTIVE**)
- È fondamentale comprendere i rischi di sicurezza associati all'ambiente IT per identificare e mitigare le potenziali vulnerabilità. È importante sviluppare sistemi resilienti che possano resistere e riprendersi rapidamente dagli incidenti di sicurezza. Ciò implica avere piani di risposta agli incidenti e strategie di recupero. (**END-TO-END SECURITY**)
- La sicurezza è una responsabilità di tutti i livelli dell'organizzazione. È importante creare una cultura della sicurezza forte, in cui tutti siano consapevoli dell'importanza della sicurezza e si impegnino a contribuire alla sua protezione. (**SECURITY BY DEFAULT**)



DMAIC: un modello per il miglioramento Continuo

D



DEFINE

Definisci il problema

M



MEASURE

Quantifica il problema

A



ANALYZE

Analizza le cause del problema

I



IMPROVE

Implementa e verifica la soluzione

C



CONTROL

Mantieni la soluzione

S . E . C . U . R . E .

Security: Priorità alla sicurezza in ogni fase dei processi aziendali. - La sicurezza deve essere una priorità assoluta per l'organizzazione, in tutte le sue fasi e processi. Deve essere integrata in modo nativo nelle attività aziendali, piuttosto che essere considerata un'aggiunta secondaria

Efficiency: Integrazione della sicurezza senza compromettere l'efficienza dei processi operativi. Le misure di sicurezza devono essere integrate nei processi aziendali senza comprometterne l'efficienza. Devono essere progettate e implementate in modo da essere compatibili con i processi esistenti e non costituire un ostacolo alla produttività

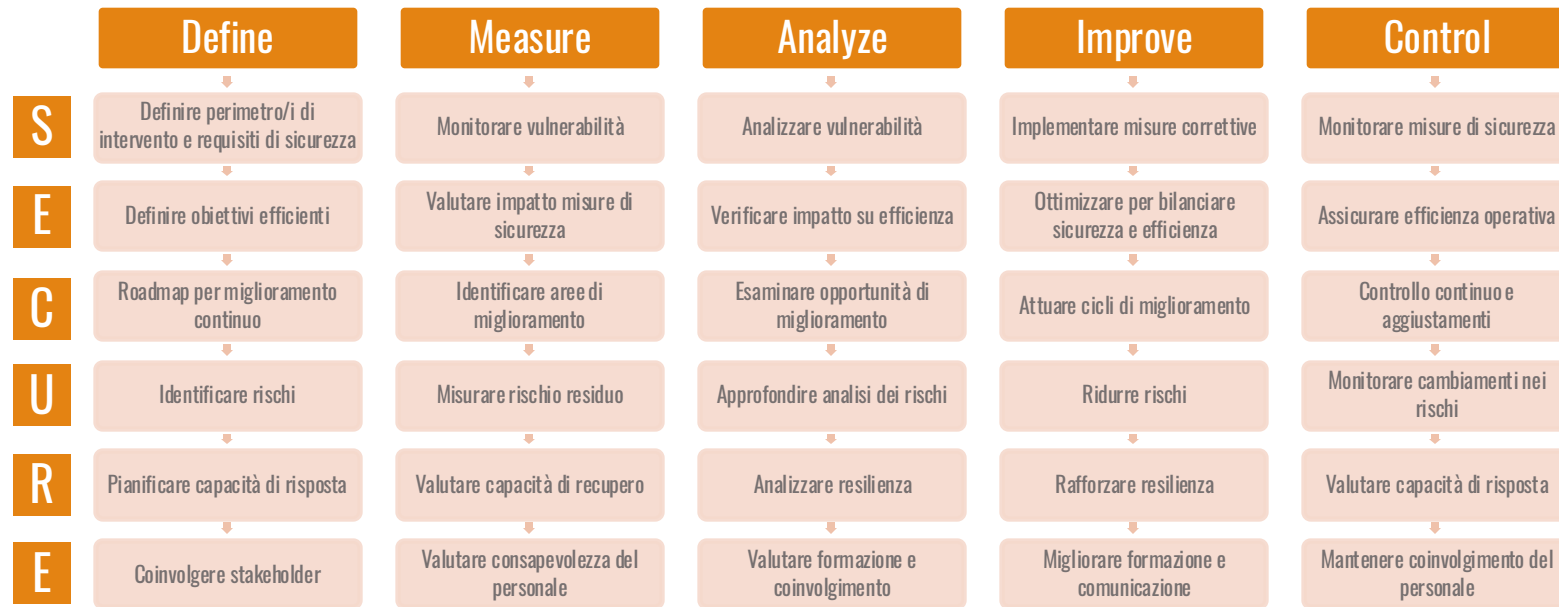
Continuous Improvement: Miglioramento continuo delle pratiche di sicurezza. Le pratiche di sicurezza devono essere migliorate costantemente per adattarsi alle mutevoli minacce e ai cambiamenti organizzativi. Devono essere periodicamente riviste e aggiornate, al fine di garantire che siano efficaci nel proteggere l'organizzazione

Understanding Risks: Comprensione approfondita dei rischi di sicurezza associati all'ambiente IT. È fondamentale comprendere i rischi di sicurezza associati all'ambiente IT per identificare e mitigare le potenziali vulnerabilità

Resilience: Sviluppo di sistemi resilienti che possano resistere e riprendersi rapidamente da incidenti di sicurezza. È importante sviluppare sistemi resilienti che possano resistere e riprendersi rapidamente dagli incidenti di sicurezza. Ciò implica avere piani di risposta agli incidenti e strategie di recupero

Engagement: Coinvolgimento attivo di tutti i livelli dell'organizzazione nella cyber security. La sicurezza è una responsabilità di tutti i livelli dell'organizzazione. È importante creare una cultura della sicurezza forte, in cui tutti siano consapevoli dell'importanza della sicurezza e si impegnino a contribuire alla sua protezione.

SECURE nel processo di miglioramento continuo



Utilizzando SECURE come guida nel DMAIC, ci si assicura che la sicurezza sia considerata una parte essenziale dell'innovazione e del miglioramento dei processi, anziché un elemento aggiuntivo

Define: Definire

Questa fase è principalmente dedicata a stabilire obiettivi chiari, comprendere il contesto del progetto, e identificare le aspettative e i requisiti.

- Stabilire chiaramente obiettivi e requisiti di sicurezza.
- Definire cosa significa “sicurezza” per il progetto specifico.
- Assicurare che gli obiettivi di sicurezza non confliggano con l'efficienza operativa.
- Considerare come la sicurezza si integrerà nei processi esistenti senza ostacolarli.
- Identificare le aree dove le pratiche di sicurezza esistenti possono essere migliorate.
- Determinare quali rischi devono essere gestiti nel contesto del progetto.
- Pianificare per la resilienza sin dall'inizio.
- Considerare come il progetto potrebbe resistere a interruzioni e attacchi.
- Stabilire come coinvolgere vari reparti e individui nel raggiungimento degli obiettivi di sicurezza.

Measure: Misurare

Il focus è sulla raccolta e l'analisi dei dati per comprendere lo stato attuale dei processi che si stanno esaminando.

- Ottenere una visione chiara della situazione attuale della sicurezza.
- Raccogliere dati specifici sulla sicurezza corrente. Questo può includere l'analisi degli incidenti di sicurezza passati, delle vulnerabilità note, e delle misure di sicurezza attualmente in atto.
- Misurare l'efficienza dei processi esistenti con particolare attenzione a come le pratiche di sicurezza attuali influenzano questa efficienza.
- Cercare di identificare eventuali punti in cui le misure di sicurezza potrebbero causare inefficienze o ritardi nei processi.
- Valutare l'efficacia delle attuali pratiche di sicurezza in termini di miglioramento continuo.
- Misurare l'adattabilità e l'agilità dei processi di sicurezza per rispondere a nuove sfide e minacce.
- Quantificare e analizzare i rischi. Ciò può includere la valutazione della frequenza e della gravità degli incidenti di sicurezza, nonché l'identificazione delle aree di maggiore rischio.
- Misurare la resilienza dei sistemi di sicurezza correnti. Questo può comportare la valutazione della capacità di ripresa dell'organizzazione dopo un incidente di sicurezza e l'efficacia dei piani di risposta agli incidenti.
- Valutare il livello di coinvolgimento e consapevolezza della sicurezza in tutta l'organizzazione. Ad esempio tramite sondaggi, interviste o analisi delle procedure di formazione e comunicazione.

Analyze: Analizzare

Esaminare in profondità i dati raccolti per identificare le cause dei problemi e le aree di miglioramento.

- Analizzare i dati di sicurezza per identificare specifiche vulnerabilità o fallimenti nei processi di sicurezza attuali.
- Cercare pattern o tendenze che indicano aree di rischio.
- Valutare come le misure di sicurezza influenzano l'efficienza operativa.
- Identificare dove le procedure di sicurezza possono essere ottimizzate per migliorare il flusso di lavoro senza diminuire la protezione.
- Identificare le aree in cui le pratiche di sicurezza possono essere migliorate.
- Analizzare i dati per trovare opportunità per rendere la sicurezza più proattiva e adattabile.
- Utilizzare i dati raccolti per avere una comprensione più dettagliata dei rischi.
- Cercare di capire la probabilità e l'impatto dei vari rischi identificati.
- Esaminare come l'organizzazione ha risposto a precedenti incidenti di sicurezza.
- Valutare la resilienza dei sistemi attuali e individua le aree che necessitano di rafforzamento per migliorare la capacità di recupero da eventi avversi.
- Analizzare il livello di coinvolgimento del personale nelle pratiche di sicurezza.
- Valutare l'efficacia delle attuali strategie di comunicazione e formazione sulla sicurezza.

Improve: Migliorare

Sviluppare e implementare soluzioni per risolvere i problemi identificati nelle fasi precedenti.

- Implementare le modifiche necessarie per colmare le lacune di sicurezza identificate. Questo potrebbe includere l'introduzione di nuove tecnologie di sicurezza, il rafforzamento delle politiche, o la correzione delle vulnerabilità scoperte.
- Assicurare che le soluzioni di sicurezza implementate siano efficienti e non compromettano il flusso di lavoro esistente.
- Cercare un equilibrio tra efficacia della sicurezza e minimizzazione dell'impatto sulle operazioni quotidiane.
- Adottare un approccio di miglioramento continuo per la sicurezza. Ciò implica l'aggiornamento e l'adattamento costante delle misure di sicurezza per rispondere a nuove minacce e cambiamenti nel contesto aziendale.
- Assicurare che le soluzioni implementate siano adeguatamente orientate a mitigare i rischi identificati.
- Valutare come le modifiche influenzano la gestione complessiva del rischio.
- Rafforzare la resilienza dei sistemi di sicurezza.
- Implementare soluzioni che non solo rispondono alle minacce attuali, ma che sono anche robuste e flessibili di fronte a sfide future.
- Coinvolgere attivamente il personale nella fase di miglioramento. Ciò può includere formazione su nuove politiche o tecnologie di sicurezza, così come il raccogliere feedback per affinare ulteriormente le strategie di sicurezza.

Control: Controllare

Monitorare e mantenere le migliorie implementate nella fase "Improve". Questa fase assicura che i cambiamenti siano sostenibili nel lungo termine e che continuino a fornire i benefici previsti.

- Monitorare costantemente le misure di sicurezza implementate per assicurare che continuino a funzionare come previsto. Ciò include il monitoraggio della conformità alle politiche di sicurezza e la verifica dell'efficacia delle nuove tecnologie o procedure.
- Assicurare che le soluzioni di sicurezza implementate continuino a operare efficientemente senza causare intoppi operativi.
- Monitorare l'impatto delle misure di sicurezza sull'efficienza dei processi aziendali.
- Valutare periodicamente le pratiche di sicurezza per identificare aree di miglioramento continuo. Questo può includere l'aggiornamento delle politiche in risposta a nuove minacce o feedback interni.
- Continuare a valutare e gestire i rischi.
- Monitorare i cambiamenti nel panorama delle minacce e adattare di conseguenza la strategia di sicurezza.
- Assicurare che i sistemi di sicurezza siano resilienti e pronti a rispondere efficacemente a eventuali incidenti. Questo include il mantenimento di piani di risposta agli incidenti aggiornati e testati.
- Mantenere un alto livello di coinvolgimento e consapevolezza della sicurezza in tutta l'organizzazione.
- Continuare a educare e informare i dipendenti sulle migliori pratiche di sicurezza e sulle politiche aziendali.



secureLean IT[®]



Grazie!

CONTATTI



[CyberSA Srl](#)



www.cybersa.it



info@cybersa.it



Via delle Conce, 20 - 00154 Roma