# SECURITY POLICY & REQUIREMENTS

# FOR

# ENGINEERING TRUSTWORTHY SECURE SYSTEM

*Autore*: *Aldo Pedico* –Cybersecurity & Privacy Consultant
*Contatto*: pedicoaldo@gmail.com

## PREMESSA

*Nell'ambito dello sviluppo di sistemi informatici più difendibili e sostenibili (inclusi i componenti meccanici, fisici e umani che compongono tali sistemi e le capacità e i servizi forniti da tali sistemi) ho voluto trattare gli aspetti che devono essere affrontati in fase progettuale della* SYSTEM SECURITY.

*Nei capitoli successivi, ho esposto un criterio che permette di approcciare alla progettazione della* SYSTEM SECURITY *in modo razionale, sia usando in modo appropriato le definizioni comunemente usate sia adottando un approccio essenziale.*

*Quindi, il mio scopo è fornire un quadro metodologico limitato a descrivere le attività delle fasi iniziali della progettazione in cui si stabiliscono le Policy all'interno delle quali si definiscono le regole, lo scopo dei controlli e i requisiti della* SYSTEM SECURITY.

*È necessario porsi l'obiettivo di affrontare i problemi della sicurezza dal punto di vista delle esigenze, delle preoccupazioni e dei requisiti di protezione delle parti interessate affinché siano affrontati con rigore adeguato durante tutto il ciclo di vita del sistema.*

# INDICE DEGLI ARGOMENTI

**Titolo** **Pag.**

# INTRODUZIONE

*La progettazione della* SYSTEM SECURITY *deve considerare:*

1) *La natura e le caratteristiche dei sistemi che informano le condizioni di definizione;*
2) *La natura e il* CONCEPT OF LOSS;
3) *Il* CONCEPT *e l'adeguatezza della* SECURITY;
4) *Il* CONCEPT OF SYSTEM SECURITY;
5) *Il* CONCEPT OF ASSET *e il ragionamento sulla* ASSET LOSS;
6) *Esigenze di protezione (Protection Needs) e vari punti di vista della sicurezza.*

*Nelle descrizioni successive, escludo volutamente il* CONCEPT OF ASSET *per motivi pratici.*

# 1 – CONCEPT OF LOSS

*La perdita è l'esperienza di avere un bene sottratto o distrutto o l'impossibilità di mantenere o continuare ad avere un bene nello stato o nella forma desiderati ed è in genere la combinazione di un evento o condizione avversa risultante e le ramificazioni, le conseguenze o gli impatti dell'evento o condizione avversa risultante.*

*La perdita è determinata e valutata indipendentemente dagli eventi e dalle condizioni causali (vale a dire, l'evento scatenante, come un errore di omissione o l'evento di sfruttamento, come un attacco).*

*Mentre la condizione o l'evento di perdita è negativo rispetto alla norma prevista, l'effetto della perdita può essere neutro/irrilevante o negativo/consequenziale.*

*La perdita può verificarsi a causa di una singola o combinazioni di cause, eventi e condizioni intenzionali e non intenzionali. Questi possono includere l'uso autorizzato o non autorizzato del sistema; atti intenzionali di disturbo o sovversione; guasti, errori e guasti umani e meccanici; atti umani di uso improprio e abuso; e il sottoprodotto dell'emergenza, degli effetti collaterali e dell'interazione delle caratteristiche.*

*Il potenziale della perdita suggerisce la necessità di obiettivi di controllo che servano come base per i giudizi sull'efficacia delle misure di protezione adottate per prevenire e limitare le perdite. Ciò include gli eventi e le condizioni avverse risultanti e le ramificazioni di tali eventi e condizioni avverse.*

*I* LOSS CONTROL OBJECTIVES *servono anche come base per acquisire prove di assicurazione che il sistema progettato, costruito, utilizzato e sostenuto proteggerà adeguatamente dalle perdite mentre raggiunge il suo intento di progettazione. Inoltre, essi riflettono l'ideale per preservare le caratteristiche delle attività (vale a dire, stato, condizione, forma, utilità) nella misura possibile nonostante il potenziale cambiamento di tali caratteristiche.*

*Gli obiettivi accettano l'incertezza sotto forma di limiti a ciò che può essere fatto (cioè,* ***non tutte le perdite possono essere evitate****) e limiti all'efficacia di ciò che viene fatto (cioè,* ***tutto ciò che viene fatto ha il suo ambito di efficacia e il suo insieme di potenziali fallimenti****).*

*Di seguito la tabella con gli Obiettivi del Controllo delle Perdite [vedi NIST SP 800-160 vol. 1]*

**TABLE 1: LOSS CONTROL OBJECTIVES**

| LOSS CONTROL OBJECTIVE | DISCUSSION |
|---|---|
| **LOSS PREVENTION** *(Prevent the loss from occurring)* | • This is the case where a loss is totally avoided. That is, despite the presence of adversity:<br>- The system continues to provide *only* the intended behavior and produces *only* the intended outcomes<br>- The desired properties of the system and assets used by the system are retained<br>- The assets continue to exist<br>• Loss avoidance may be achieved by any combination of:<br>- Preventing or removing the event or events that cause the loss (**the loss never occurs**)<br>- Preventing or removing the condition or conditions that allow the loss to occur (**the loss never occurs**)<br>- Not suffering an adverse effect despite the events or conditions (**the loss never occurs**)<br>• Terms such as *avoid, continue, delay, divert, eliminate, harden, prevent, redirect, remove, tolerate,*[25] *and withstand* are typically used to characterize approaches to achieve this objective such that a loss does not occur despite the system being subjected to adversity |
| **LOSS LIMITATION** *(Limit the extent of the loss)* | • This covers cases where a loss can or has occurred, and the extent of loss is to be limited<br>• The extent of loss can be limited in terms of any combination of the following:<br>- Limited dispersion (e.g., migration, propagation, spreading, ripple, domino, or cascading effects)<br>- Limited duration (e.g., milliseconds, minutes, hours, days)<br>- Limited capacity (e.g., diminished utility, delivery of function, service, or capability)<br>- Limited volume (e.g., bits or bytes of data/information)<br>• Decisions to limit the extent of loss may require prioritizing what constitutes acceptable loss across a set of losses, whereby the objective to limit the loss for one asset requires accepting a loss of some other asset<br>• The extreme case of loss limitation is to avoid destruction of the asset<br>• Terms such as *tolerate, withstand, remove, continue, constrain, stop/halt,* and *restart* fall into this category in the case where the loss occurs and the system can, or enables the ability to, limit the effect of the loss |
| **LOSS CONTROL OBJECTIVE** | **DISCUSSION** |
| | • Loss recovery and loss delay are two means to limit loss:<br>- *Loss Recovery:* Action is taken by the system or enabled by the system to recover (or allow the recovery of) some or all of its ability to function (i.e., behave, interact, produce outcomes) and to recover assets used by the system (e.g., re-imaging, reloading, or recreating information and data, including software in the system). The restoration of the asset, fully or partially, can limit the dispersion, duration, capacity, or volume of the loss.<br>- *Loss Delay:* The loss event is avoided until the adverse effect is lessened or when a delay enables a more robust response or quicker recovery.<br>• System and environmental conditions may be assumed to result in loss, but measures are taken to limit impacts<br>• Terms such as *contain, recover, restore, reconstitute, reconfigure,* and *restart* are typically used to characterize approaches to achieving this objective |

# 2 – CONCEPT OF SECURITY

*Un sistema libero dalle condizioni che possono causare una perdita di beni con conseguenze inaccettabili deve fornire i comportamenti e i risultati previsti (ad esempio, la funzionalità del sistema prevista) ed evitare comportamenti e risultati non intenzionali che costituiscono una perdita.*

*Il termine inteso ha due casi da soddisfare entrambi:*

1) INTENTO PROGETTUALE: *come previsto dal progetto;*
2) INTENTO DELL'UTENTE: *come previsto dall'utente.*

**L'obiettivo principale della sicurezza è garantire che si verifichino solo i comportamenti e i risultati previsti, sia con il sistema sia al suo interno del sistema.**

*Ogni esigenza e preoccupazione di sicurezza deriva da questo obiettivo, che si basa sul* CONCEPT OF AUTHORIZATION *per ciò che è e non è consentito.*

*In quanto tale,* **l'obiettivo principale del controllo di sicurezza è l'applicazione di vincoli sotto forma di regole per comportamenti e risultati consentiti e non consentiti**.

*Questo obiettivo di controllo della sicurezza, nonché uno dei principi fondamentali di una progettazione sicura e affidabile, è l'accesso mediato.*

**Se l'accesso non è mediato (vale a dire, controllato attraverso l'applicazione di vincoli) in conformità con una serie di regole non in conflitto, non vi è alcuna base su cui rivendicare il raggiungimento della sicurezza.**

*Le regole per l'accesso mediato sono stabilite in una serie di* POLITICHE DI SICUREZZA *che riflettono o derivano da leggi, direttive, regolamenti, concetti del ciclo di vita, requisiti o altri obiettivi delle parti interessate specificatamente dichiarati.*

*Ciascun criterio di sicurezza include un ambito di controllo che stabilisce i limiti entro i quali si applica il criterio.*

*Le regole della politica di sicurezza sono stabilite in termini di* ***soggetti (entità attive)****,* ***oggetti (entità passive)*** *e operazioni che il soggetto può eseguire o invocare sull'oggetto.*

*Le regole per ciascuna politica di sicurezza devono essere accurate, coerenti, compatibili e complete rispetto agli obiettivi degli stakeholder nell'ambito del controllo.*

**Affinché un sistema sia considerato affidabile e sicuro, deve esserci sufficiente certezza che il sistema sia in grado di applicare la POLITICA DI SICUREZZA su base continua per la durata del tempo in cui la POLITICA DI SICUREZZA è in vigore.**

## 3 – CONCEPT OF SYSTEM SECURITY

*La definizione di sicurezza può essere interpretata per catturare cosa si intende per sistema sicuro.*

**Un sistema sicuro è un sistema che, per tutti i suoi stati, modalità e transizioni identificati, garantisce che si verifichino solo i comportamenti e i risultati previsti autorizzati, fornendo così libertà da quelle condizioni, sia intenzionalmente/con malizia che non intenzionalmente/senza malizia, che possano causare una perdita di beni con conseguenze inaccettabili.**

*Questa definizione esprime un ideale che coglie i tre aspetti essenziali di cosa significa raggiungere la sicurezza:*

1) *Consentire la fornitura della capacità di sistema richiesta nonostante forme di avversità intenzionali e non intenzionali;*
2) *Applicare i vincoli per garantire che solo i comportamenti e i risultati desiderati associati alla capacità del sistema richiesta siano realizzati soddisfacendo il primo aspetto;*

3) *Applicare vincoli basati su una serie di regole per garantire che solo le interazioni e le operazioni H-M e M-M autorizzate possano verificarsi soddisfacendo il secondo aspetto.*

*Per un sistema, una sicurezza adeguata è una determinazione basata sull'evidenza che raggiunge e ottimizza le prestazioni di sicurezza rispetto a tutti gli altri obiettivi e vincoli di prestazioni.*

*I giudizi di sicurezza adeguata sono guidati dagli obiettivi, dai bisogni e dalle preoccupazioni degli stakeholder associati al sistema.*

*Una sicurezza adeguata ha due elementi:*

1) *Il raggiungimento della soglia minima accettabile di prestazione della sicurezza;*
2) *La massimizzazione delle prestazioni di sicurezza nella misura in cui qualsiasi ulteriore aumento delle prestazioni di sicurezza si traduce in un degrado di qualche altro aspetto delle prestazioni del sistema o richiede un impegno operativo inaccettabile.*

**Infine, la sicurezza adeguata è determinata in base al punto di vista, al contesto, alla criticità e alla priorità e può variare a seconda della missione o degli obiettivi operativi aziendali o tra gli stati e le modalità del sistema così come esiste (ad esempio, operazione, stoccaggio o transito).**

# 4 – SECURITY POLICY

**Una POLITICA DI SICUREZZA è un insieme di regole che governa il comportamento all'interno di un ambito di controllo definito.**

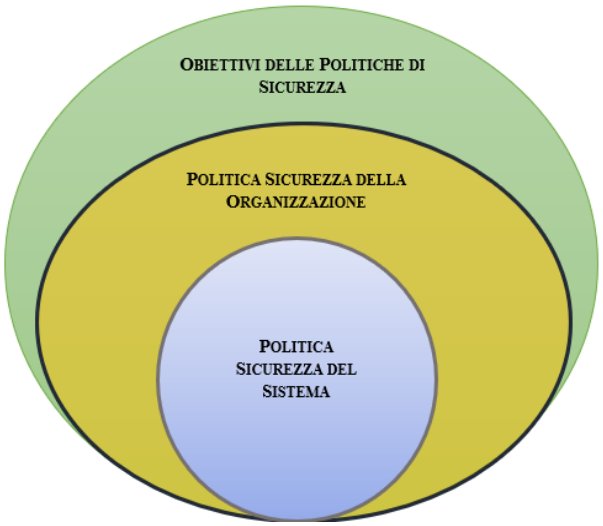
*Il termine "*POLITICA DI SICUREZZA*" viene utilizzato in diversi modi, tra cui:*

1) **OBIETTIVI della POLITICA di SICUREZZA,**
2) **POLITICA di SICUREZZA ORGANIZZATIVA,**
3) **POLITICA di SICUREZZA del SISTEMA.**

*Le* POLITICHE DI SICUREZZA *hanno una varietà di contesti, autorità, ambiti e scopi e <u>in genere formano relazioni gerarchiche</u>.*

*Ad esempio: gli* OBIETTIVI DELLE POLITICHE DI SICUREZZA *comprendono la* POLITICA *di* SICUREZZA DELL'ORGANIZZAZIONE, *che a sua volta include la* POLITICA *di* SICUREZZA *del* SISTEMA.

INSIEME DELLE SECURITY POLICY



## 4.1 - RULES

Le regole della politica di sicurezza sono stabilite in termini di soggetti (cioè **entità attive**), oggetti (cioè **entità passive**) e operazioni che i soggetti possono eseguire o invocare sugli oggetti.

Le regole per ciascuna politica di sicurezza governano i comportamenti e gli esiti da soggetto a oggetto.

Le regole devono essere accurate, coerenti, compatibili e complete rispetto agli obiettivi degli stakeholder per l'ambito di controllo definito.

*In caso contrario, si verificheranno delle lacune nel comportamento governato desiderato.*

## 4.2 – SCOPE OF CONTROL

Le politiche di sicurezza riflettono e derivano da leggi, direttive, regolamenti, concetti del ciclo di vita, requisiti o obiettivi degli stakeholder.

*Ciascun criterio di sicurezza include un ambito di controllo che stabilisce i limiti entro i quali si applica il criterio.*

*Gli* **OBIETTIVI** *della* **POLITICA** *di* **SICUREZZA**, *la* **POLITICA** *di* **SICUREZZA** *dell'***ORGANIZZAZIONE** *e la* **POLITICA** *di* **SICUREZZA** *del* **SISTEMA** *hanno in genere un ambito di applicabilità specifico come segue:*

- ✓ SECURITY POLICY (PROTECTION) OBJECTIVES

  *Gli obiettivi politici catturano ciò che deve essere raggiunto o uno stato preferito.*

  *Gli obiettivi della politica di sicurezza includono:*

  1) *le risorse da proteggere,*
  2) *una dichiarazione di intenti per proteggere le risorse nell'ambito specifico della responsabilità degli stakeholder e*
  3) *l'ambito delle protezioni.*

  *Gli* **OBIETTIVI** *della* **POLITICA** *di* **SICUREZZA** *sono la base per la derivazione di tutte le altre forme di politica di sicurezza.*

- ✓ ORGANIZATIONAL SECURITY POLICY

  *La* **POLITICA** *di* **SICUREZZA** *dell'***ORGANIZZAZIONE** *è "L'INSIEME DI REGOLE CHE DISCIPLINANO IL MODO IN CUI UN'ORGANIZZAZIONE RAGGIUNGE I PROPRI OBIETTIVI".*

  *Per essere significative, le regole forniscono alle persone una ragionevole capacità di determinare se le loro azioni violano o rispettano la politica.*

*La* **POLITICA** *di* **SICUREZZA** *dell'***ORGANIZZAZIONE** *definisce "IL COMPORTAMENTO DELLE PERSONE NELLO SVOLGIMENTO DELLE LORO MISSIONI E FUNZIONI AZIENDALI" ed è utilizzata per lo sviluppo di processi e procedure.*

✓ SYSTEM SECURITY POLICY

*La* **POLITICA** *di* **SICUREZZA** *del* **SISTEMA** *specifica "COSA DOVREBBE FARE LA CAPACITÀ DI SICUREZZA DEL SISTEMA".*

*È l'insieme di restrizioni e proprietà che specifica come un sistema applica o contribuisce all'applicazione di una* **POLITICA** *di* **SICUREZZA** *dell'***ORGANIZZAZIONE**.

*La* SECURITY POLICY *passa attraverso un processo di raffinamento iterativo che scompone una dichiarazione astratta di politica di sicurezza in dichiarazioni più specifiche di politica di sicurezza. Ciò avviene parallelamente all'allocazione dei requisiti di sicurezza e alla scomposizione dei requisiti man mano che la progettazione del sistema matura.*

*La figura C-1 illustra l'allocazione delle politiche di sicurezza nell'organizzazione.*

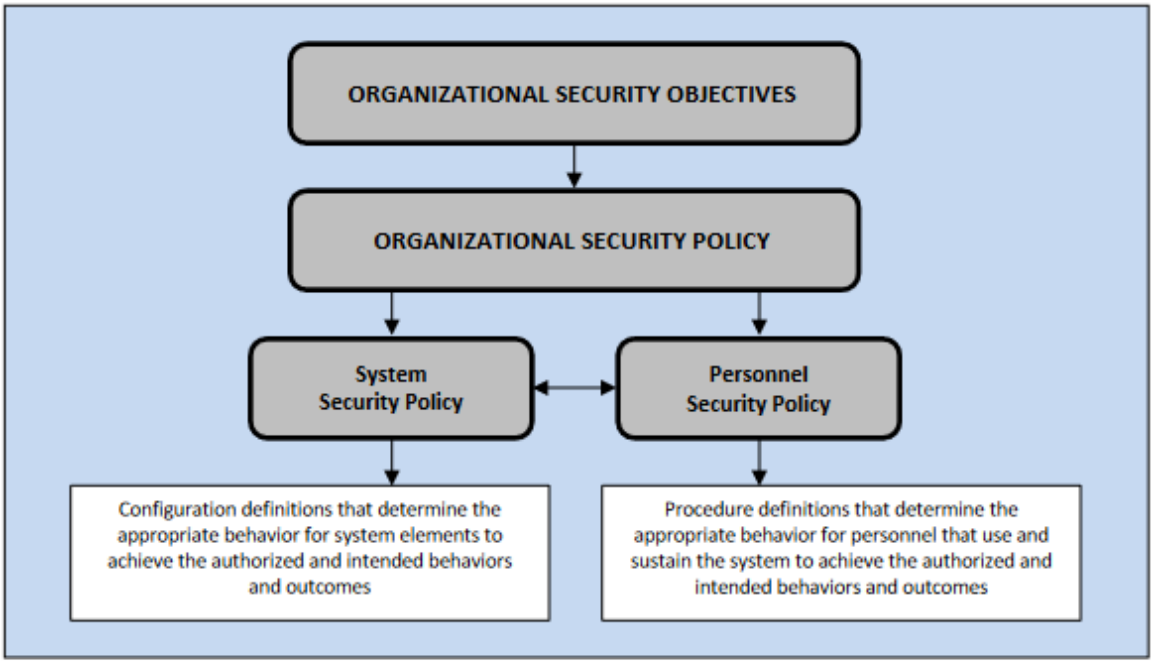



**FIGURE C-1: ALLOCATION OF SECURITY POLICY RESPONSIBILITIES**

ASSEGNAZIONE DELLE RESPONSABILITÀ DELLA POLITICA DELLA SECURITY

# 5 – REQUIREMENTS

## Definizione di Requisito

*"Un requisito è un'affermazione che traduce o esprime un'esigenza specifica e i vincoli e le condizioni associati" [ISO 29148].*

*I requisiti di sicurezza traducono o esprimono esigenze di protezione, vincoli associati e condizioni associate.*

*I vincoli riflettono anche le preoccupazioni relative alle funzioni del sistema, all'architettura del sistema e alla progettazione per garantire che siano specificati in modo da evitare e ridurre suscettibilità, difetti, imperfezioni e debolezze ed è coerente con le esigenze di funzioni di sicurezza.*

*I requisiti possono essere classificati come:*

1) REQUISITI DELLE PARTI INTERESSATE [STAKEHOLDER REQUIREMENTS] *che affrontano la necessità di essere soddisfatti in modo indipendente dalla progettazione; e*
2) REQUISITI DI SISTEMA [SYSTEM REQUIREMENTS] *che esprimono la soluzione specifica che verrà fornita (modo design-dependent).*

*La figura C-2 illustra i due tipi di requisiti e la loro relazione con la verifica e la validazione del sistema.*

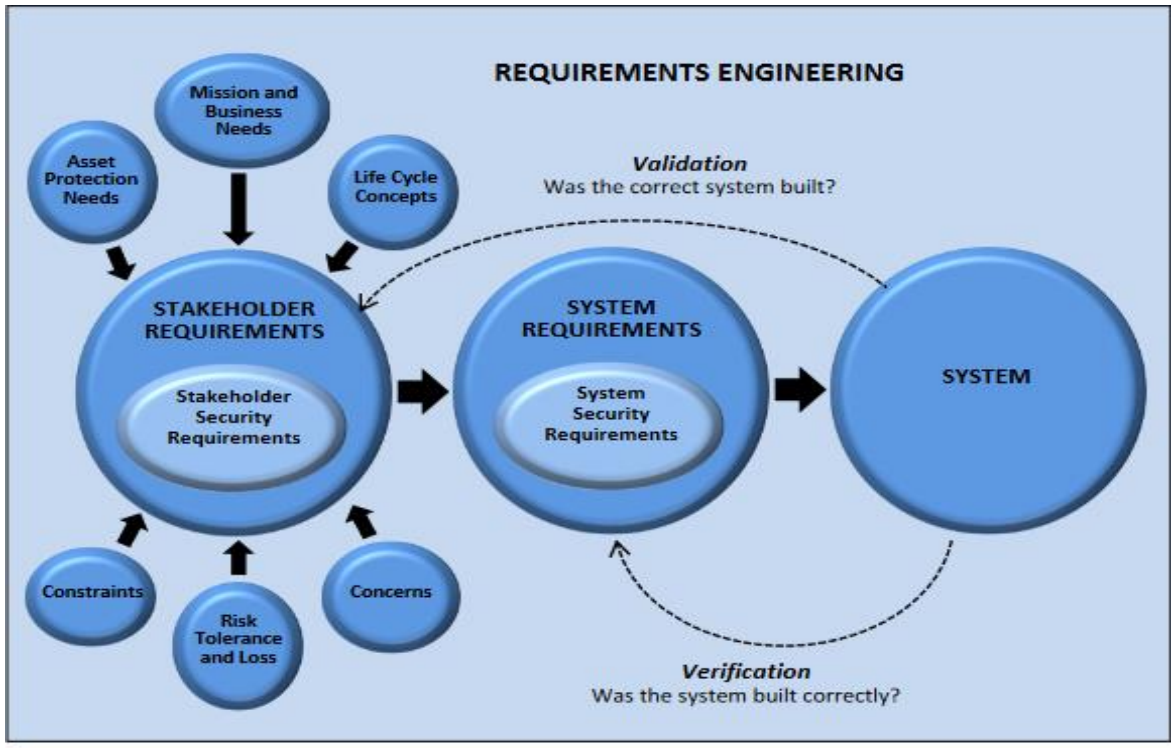



**FIGURE C-2: STAKEHOLDER AND SYSTEM REQUIREMENTS**

*I requisiti di sicurezza, i vincoli e le condizioni rilevanti per la sicurezza su altri requisiti sono informati da vari elementi, come quelli illustrati nella Figura C-3.*

## 5.1 - STAKEHOLDER SECURITY REQUIREMENTS

*I requisiti di sicurezza degli stakeholder sono quei requisiti degli stakeholder rilevanti per la sicurezza.*

*I requisiti di sicurezza delle parti interessate specificano:*

1) *La protezione necessaria per la missione o l'azienda, dati, informazioni, processi, funzioni, persone e risorse di sistema.*
2) *I ruoli, le responsabilità e le azioni rilevanti per la sicurezza delle persone che svolgono e supportano la missione oi processi aziendali.*
3) *Le interazioni tra gli elementi della soluzione rilevanti per la sicurezza.*
4) *L'assicurazione che deve essere ottenuta nella soluzione di sicurezza.*

*Le considerazioni sulla sicurezza dei sistemi nell'ambito delle attività e delle attività (come quelle descritte nel Capitolo tre) forniscono la prospettiva di sicurezza per garantire che i requisiti di sicurezza appropriati degli stakeholder siano inclusi nei requisiti degli stakeholder e che gli stakeholder i requisiti di sicurezza sono coerenti con tutti gli altri requisiti delle parti interessate.*

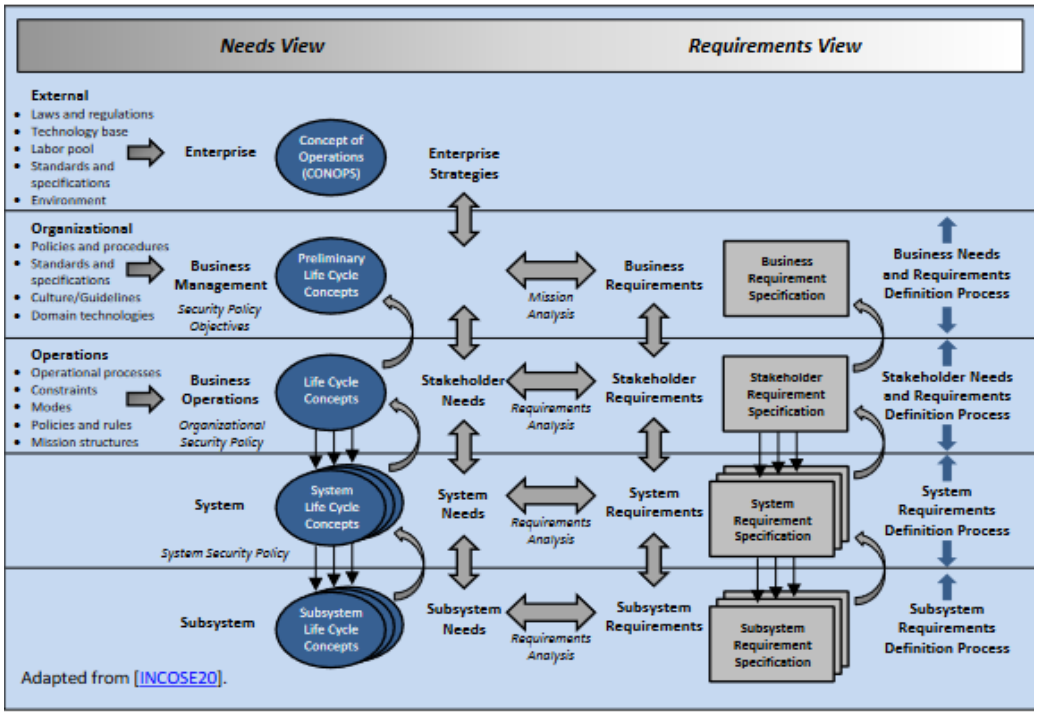



**FIGURE C-3: ENTITIES THAT AFFECT SECURITY REQUIREMENT DEVELOPMENT**

## 5.2 – SYSTEM SECURITY REQUIREMENTS

*I requisiti di sistema specificano la vista tecnica di un sistema o di una soluzione che soddisfi le esigenze delle parti interessate specificate.*

*I requisiti di sistema sono una trasformazione dei requisiti degli stakeholder convalidati.*

*I requisiti di sistema specificano cosa deve fare il sistema o la soluzione per soddisfare i requisiti degli stakeholder.*

**I requisiti di sicurezza del sistema sono quei requisiti di sistema rilevanti per la sicurezza.**

**Questi requisiti definiscono:**

1) **Le capacità di protezione fornite dalla soluzione di sicurezza;**
2) **Le caratteristiche prestazionali e comportamentali esibite dalla soluzione di sicurezza;**
3) **I processi, le procedure e le tecniche di assicurazione;**
4) **I vincoli sul sistema e sui processi, i metodi e gli strumenti utilizzati per realizzare il sistema;**
5) **Le prove richieste per determinare i requisiti di sicurezza del sistema sono state soddisfacenti.**

**A causa della complessità della sicurezza del sistema, esistono diversi tipi e scopi di requisiti di sicurezza del sistema.**

**Questi includono:**

1) **i requisiti di sicurezza strutturale che esprimono gli aspetti passivi della capacità di protezione fornita dall'architettura del sistema, e**
2) **i requisiti di sicurezza funzionale che esprimono gli aspetti attivi della capacità di protezione fornita da caratteristiche e dispositivi ingegnerizzati (es. meccanismi di sicurezza, controlli, salvaguardie, inibizioni, override e contromisure).**

*La scomposizione dei requisiti di sicurezza del sistema viene eseguita come parte della scomposizione dei requisiti di sistema e deve essere coerente con i diversi livelli di astrazione gerarchica e le forme dei requisiti di sistema.*

## 6 – SYSTEM STATES — SECURE AND NON SECURE

*I sistemi una volta implementati avranno stati che possono essere sicuri o non sicuri.*

*La politica e i requisiti riflettono questi stati.*

*La definizione di sicurezza è stata interpretata per cogliere cosa si intende per sistema sicuro:*

**"Un sistema sicuro è un sistema che, per tutti i suoi stati, modalità e transizioni identificati, garantisce che accadano solo comportamenti e risultati autorizzati, liberando così quelle condizioni, sia intenzionali/con dolo che non intenzionali/senza dolo, che possano causare una perdita di beni con conseguenze inaccettabili".**

*Questa interpretazione esprime un ideale che coglie gli aspetti essenziali di cosa significa raggiungere la sicurezza del sistema.*

*Questi aspetti includono:*

1) CONSENTIRE [ENABLING] *l'erogazione della capacità richiesta nonostante forme di avversità intenzionali e non intenzionali.*
2) APPLICARE [ENFORCING] *i vincoli per garantire che solo i comportamenti e i risultati desiderati associati alla capacità richiesta siano realizzati soddisfacendo il primo aspetto.*
3) APPLICARE [ENFORCING] *i vincoli sulla base di un insieme di regole per garantire che solo le interazioni e le operazioni autorizzate* Uomo-Macchina *e* Macchina-Macchina *siano consentite soddisfacendo il secondo aspetto.*

**La politica di sicurezza del sistema e i requisiti di sistema esprimono che l'insieme di tutti i possibili stati del sistema possa essere suddiviso sia nell'insieme degli stati sicuri (ovvero quali stati sono consentiti) sia nell'insieme degli stati non sicuri (cioè quali stati non sono consentiti).**

*Un sistema sicuro è, quindi, un sistema che inizia l'esecuzione in uno stato sicuro e non può passare a uno stato non sicuro.*

*Ovvero, ogni transizione di stato si traduce nello stesso stato protetto o in un altro stato protetto.*

*Ogni transizione di stato deve anche essere sicura.*

*La Figura C-4 illustra queste transizioni di stato del sistema sicuro "idealizzato".*

*Sebbene sia teoricamente possibile progettare un sistema così idealizzato, non è pratico farlo.*

*Pertanto, le politiche e i requisiti di sicurezza dovrebbero includere stati aggiuntivi e transizioni di stato di supporto che riflettano i principi chiave di* PROTECTIVE FAILURE *e* PROTECTIVE RECOVERY.

*Il guasto protettivo richiede la capacità di:*

1) *rilevare che il sistema è in uno stato non sicuro;*
2) *rilevare una transizione che porrà il sistema in uno stato non sicuro per evitare la propagazione di nuovi guasti.*

*Il guasto protettivo richiede azioni reattive e correttive.*

*Include il passaggio a uno stato di arresto sicuro con un ripristino protetto per consentire la continuazione delle operazioni in una modalità operativa sicura ricostituita, riconfigurata o alternativa.*

*Altri obiettivi delle parti interessate possono anche richiedere la continuazione delle operazioni in uno stato non completamente sicuro.*

*La politica e i requisiti dovrebbero riflettere tali necessità.*

*Il ripristino protettivo richiede la capacità di effettuare azioni reattive, reattive o correttive per passare in modo sicuro da uno stato non sicuro a uno stato sicuro (o meno insicuro).*

*Lo stato di sicurezza raggiunto dopo il completamento delle azioni di ripristino della protezione include quelle azioni che limitano o impediscono qualsiasi ulteriore transizione di stato e quelle che costituiscono un tipo di modalità, operazione o capacità degradate.*

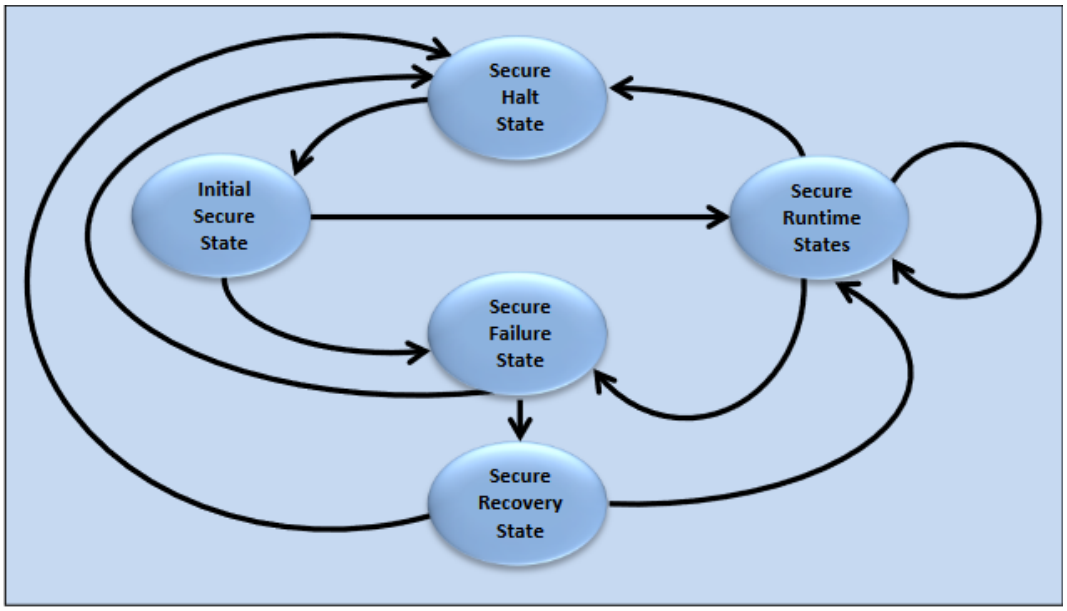



**FIGURE C-4: IDEALIZED SECURE SYSTEM STATE TRANSITIONS**

# 7 - DISTINGUISHING REQUIREMENTS, POLICY, AND MECHANISMS

*I termini* ***requisiti***, ***politica*** *e* ***meccanismi*** *sono spesso usati in modi astratti che consentono di considerarli come sinonimi.*

*Tuttavia, quando utilizzati nel contesto della progettazione di sistemi sicuri affidabili, questi termini sono distinti nel loro significato e importanza per* ***specificare***, ***realizzare***, ***utilizzare*** *e* ***sostenere*** *i sistemi in modo sicuro e affidabile.*

**La POLITICA DELLA SICUREZZA (È IL CHE COSA) "***STABILISCE IL COMPORTAMENTO NECESSARIO PER***" raggiungere una condizione di sicurezza, mentre un MECCANISMO DI SICUREZZA (È IL COME) è "***UN MEZZO PER***" ottenere il comportamento necessario.**

*La distinzione tra* **POLITICA DELLA SICUREZZA** *e* **MECCANISMO DI SICUREZZA** *si estende alla* **DIFFERENZIAZIONE** *dei* REQUISITI *di* SICUREZZA *dalla* POLITICA DELLA SICUREZZA.

*I* **REQUISITI DI SICUREZZA** *specificano la capacità, il comportamento e gli attributi di qualità mostrati e posseduti dai meccanismi di sicurezza, nonché i vincoli su ciascuno.*

*La* **POLITICA DELLA SICUREZZA** *specifica come devono comportarsi i* **MECCANISMI DI SICUREZZA** *in un determinato contesto operativo e i vincoli su tali comportamenti.*

*Dal punto di vista del sistema, un essere umano è un elemento del sistema e può fungere da meccanismo di sicurezza.*

*Pertanto, ci si aspetta che l'essere umano si comporti come indicato dalla politica di sicurezza pertinente e dai requisiti di sicurezza.*

*Requisiti, politiche e meccanismi hanno un'importante relazione di dipendenza.*

*I* **SYSTEM SECURITY REQUIREMENTS** *del sistema specificano le capacità ei comportamenti che un meccanismo di sicurezza è in grado di fornire.*

*Una* **SECURITY POLICY** *specifica gli aspetti particolari che un meccanismo deve applicare per raggiungere gli* **ORGANIZATIONAL OBJECTIVES**.

*Ciò significa che non è possibile ottenere un sistema sicuro se i requisiti di sicurezza non specificano completamente la capacità minima necessaria per far rispettare la politica di sicurezza.*

*Significa anche che la sola soddisfazione dei requisiti non si traduce in un sistema sicuro.*

*Le attività di verifica e validazione devono essere svolte separatamente e coordinate per garantire la correttezza e l'efficacia individuale e combinata dei requisiti e della politica.*

*La Figura C-5 illustra il significato della relazione di coerenza che deve essere mantenuta tra i requisiti di sicurezza, i criteri di sicurezza e i meccanismi di sicurezza interagenti.*

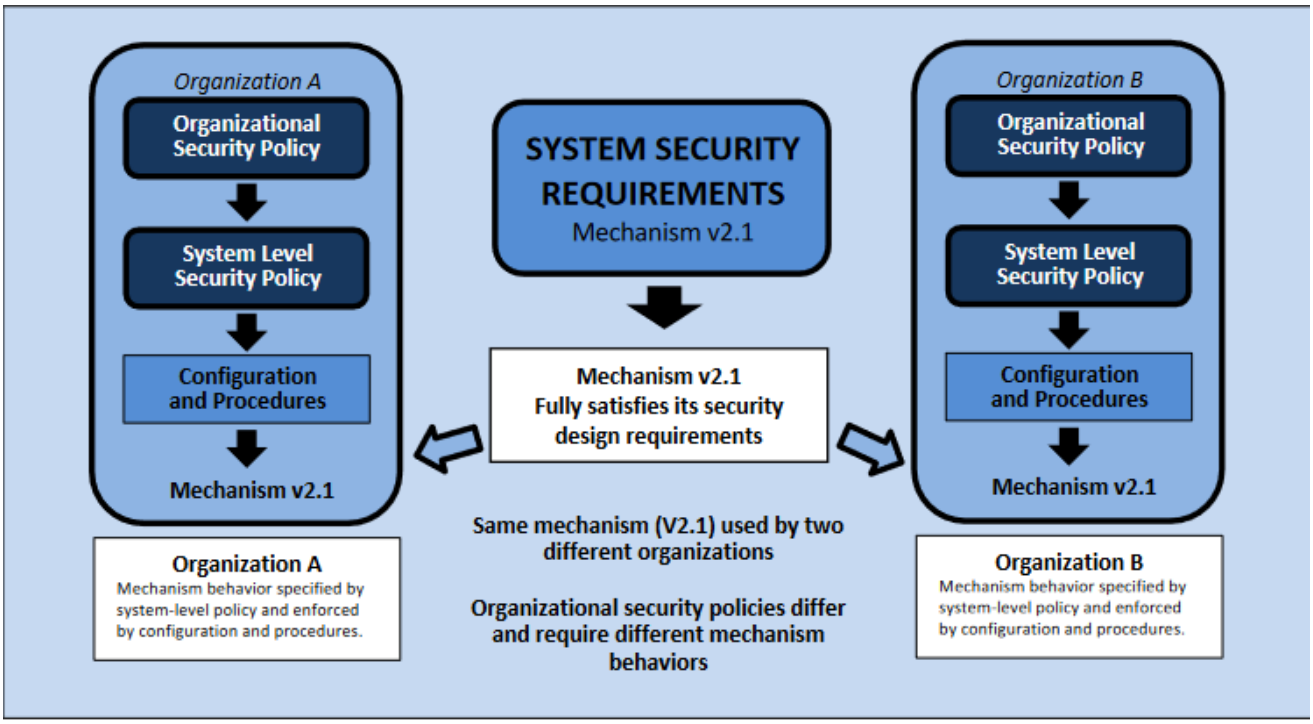



**FIGURE C-5: RELATIONSHIP BETWEEN MECHANISMS AND SECURITY POLICY ENFORCEMENT**

*Qualsiasi meccanismo di sicurezza che soddisfi pienamente i requisiti di sicurezza del sistema può essere ritenuto in grado di applicare la politica di sicurezza definita per due diverse organizzazioni.*

*Ciascuna organizzazione utilizzerà lo stesso meccanismo e lo configurerà in modo che si comporti in modo da applicare le regole della propria politica di sicurezza organizzativa.*

*Tuttavia, se le organizzazioni dovessero cambiare meccanismo e mantenere la stessa configurazione del meccanismo, otterrebbero risultati incerti (a meno che i loro obiettivi della politica di sicurezza non richiedano esattamente la stessa configurazione del meccanismo).*

## 7.1 - CONCLUSIONI

Da quanto precedentemente descritto, si possono trarre le seguenti conclusioni:

1) **I REQUIREMENTS determinano la CAPABILITY dei SECURITY MECHANISMS;**
2) **La SECURITY POLICY determina il BEHAVIOR (COMPORTAMENTO) ritenuto "sicuro".**
3) **Affinché un MECHANISM sia considerato sicuro:**
    a) **i REQUIREMENTS per la CAPABILITY del meccanismo devono essere coerenti con le regole di applicazione della SECURITY POLICY;**
    b) **il MECHANISM deve soddisfare i SECURITY REQUIREMENTS;**
    c) **il MECHANISM deve essere configurato per comportarsi nel modo definito dall'ORGANIZATIONAL SECURITY POLICY.**

## RIFERIMENTI

*1)* NIST SP 800-160 - vol1 NIST SP 800-160 - vol1 Engineering Trustworthy Secure System