Le Criticità dei Sistemi Informatici

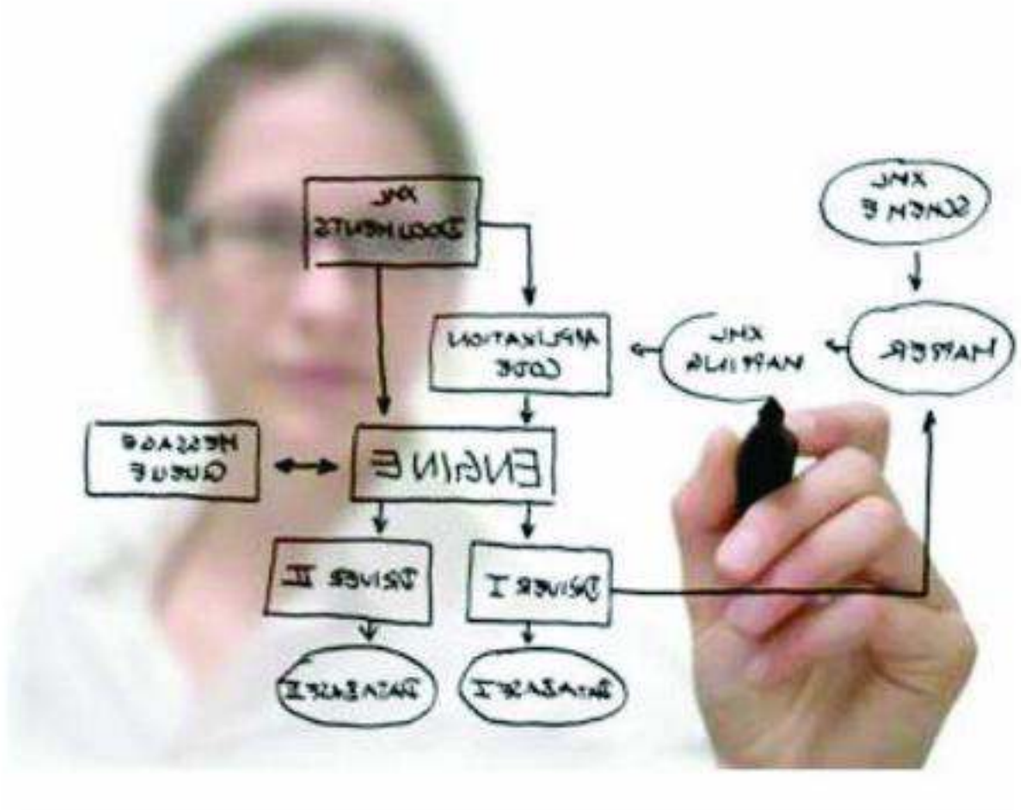
COSA SI INTENDE PER SISTEMA INFORMATICO?

Per sistema informatico intendiamo un insieme di computer (hardware + software) che elaborano dati e informazioni per produrre altri dati ed informazioni utili.
Per non creare confusione teniamo presente che le definizioni Sistema Informatico e Sistema Informativo non si equivalgono: il Sistema Informativo è l'insieme delle attività di gestione delle informazioni, delle relative modalità e degli strumenti tecnologici usati a tale scopo. Ne consegue quindi che il Sistema Informatico ne costituisce soltanto una parte.

*Anche il più semplice dei computer può in teoria essere definito **sistema** essendo necessaria al suo funzionamento la combinazione di hardware e software, tuttavia il termine 'sistema' in informatica ha significato solo quando sono presenti interconnessioni fra computer diversi che, insieme, formano un sistema più grande.*
L'intrinseca complessità dei sistemi informatici, dovuta alla sovrapposizione di più strati di hardware e software e all'interazione che alcuni sistemi hanno con input provenienti da decisioni umane, produce una quantità enorme di variabili che non consentono la formalizzazione "matematica" delle relazioni causa-effetto tra gli input e gli output.
Questo ci obbliga a soffermarci sull'importanza di "tutelare" il sistema informatico come parte integrante del sistema informativo definendo strategie adatte al livello di criticità che il sistema stesso ricopre.

CICLO DI VITA DELLO SVILUPPO DEI SISTEMI (SDLC)

SDLC ANALISI DEI REQUISITI



Lo scopo della fase di analisi dei requisiti è di determinare che cosa il sistema in questione deve fare.
Attraverso la negoziazione fra gli analisti e i clienti si cerca di comprendere i reali bisogni e di ottenere la soddisfazione delle necessità tendo conto della disponibilità di mezzi (economici, umani, tecnologici, etc..)

SDLC PROGETTAZIONE

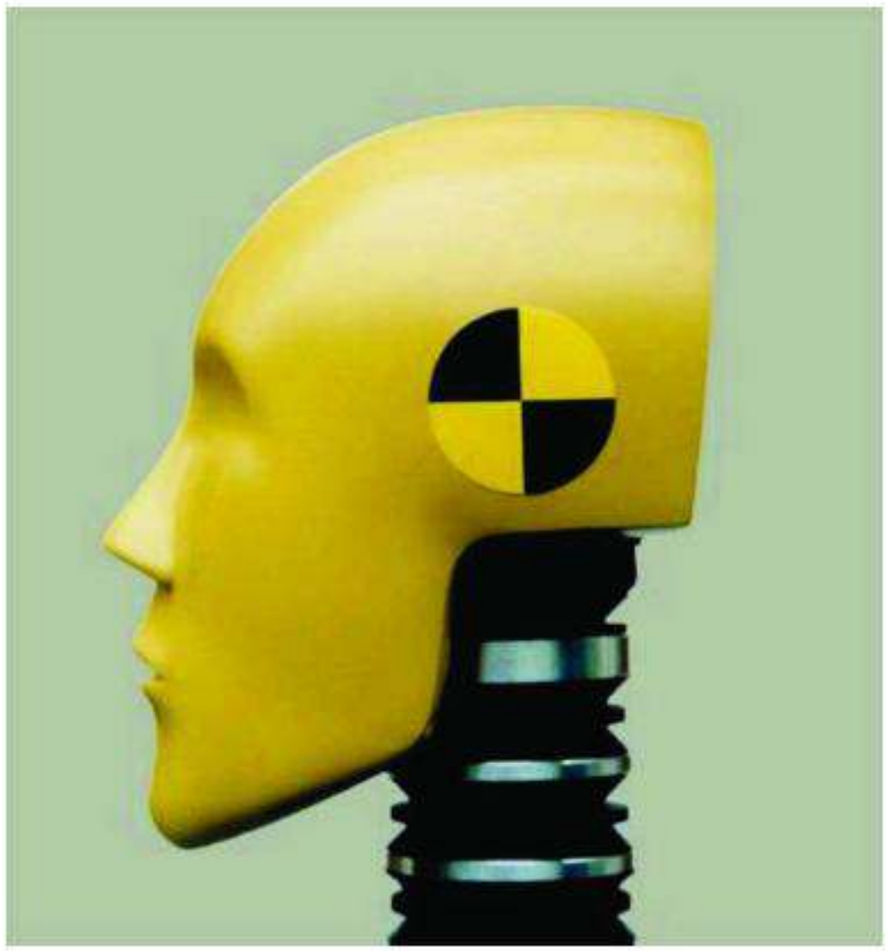
Durante questa fase, detta anche di design, si progetta il sistema in dettaglio, si stabiliscono i ruoli, i diagrammi di processo, le gerarchie e tutto quanto necessario a fare in modo che durante la successiva fase di implementazione non sopraggiungano dubbi o problematiche prevedibili.
Questa è senza dubbio la fase che richiede più attenzione.

SDLC IMPLEMENTAZIONE

A questo punto è giunto il momento di mettere insiemi i pezzi del puzzle.
I vari componenti del sistema entrano in relazione tra loro.
Se le fasi precedenti sono state svolte correttamente sarà più agevole mettere in opera il sistema che potrà definirsi così pronto per affrontare la prossima fase, quella cruciale.

SDLC

TESTING



Il momento della verità.

Il sistema viene stressato attraverso l'utilizzo di diverse tecniche e metodologie mirate ad evidenziarne le eventuali falle o lacune per consentirne la messa a punto ed evitare che possa dimostrarsi inadatto a svolgere la sua funzione.

LA GESTIONE DEL RISCHIO

Un'efficace gestione del rischio (Risk Management) deve essere totalmente integrata nella SDLC e come processo iterativo può essere implementato durante ciascuna delle 5 fasi.

Il Risk Management si compone principalmente di 2 fasi:

- Valutazione del rischio (Risk Assessment)
- Mitigazione del rischio (Risk Mitigation)

VALUTAZIONE DEL RISCHIO

In questa fase (chiamata anche in letteratura tecnica "analisi del rischio") vanno determinati, analizzati e classificati i rischi e vanno stimate le vulnerabilità del sistema, in modo che sia poi possibile individuare le salvaguardie più adeguate ed efficaci.

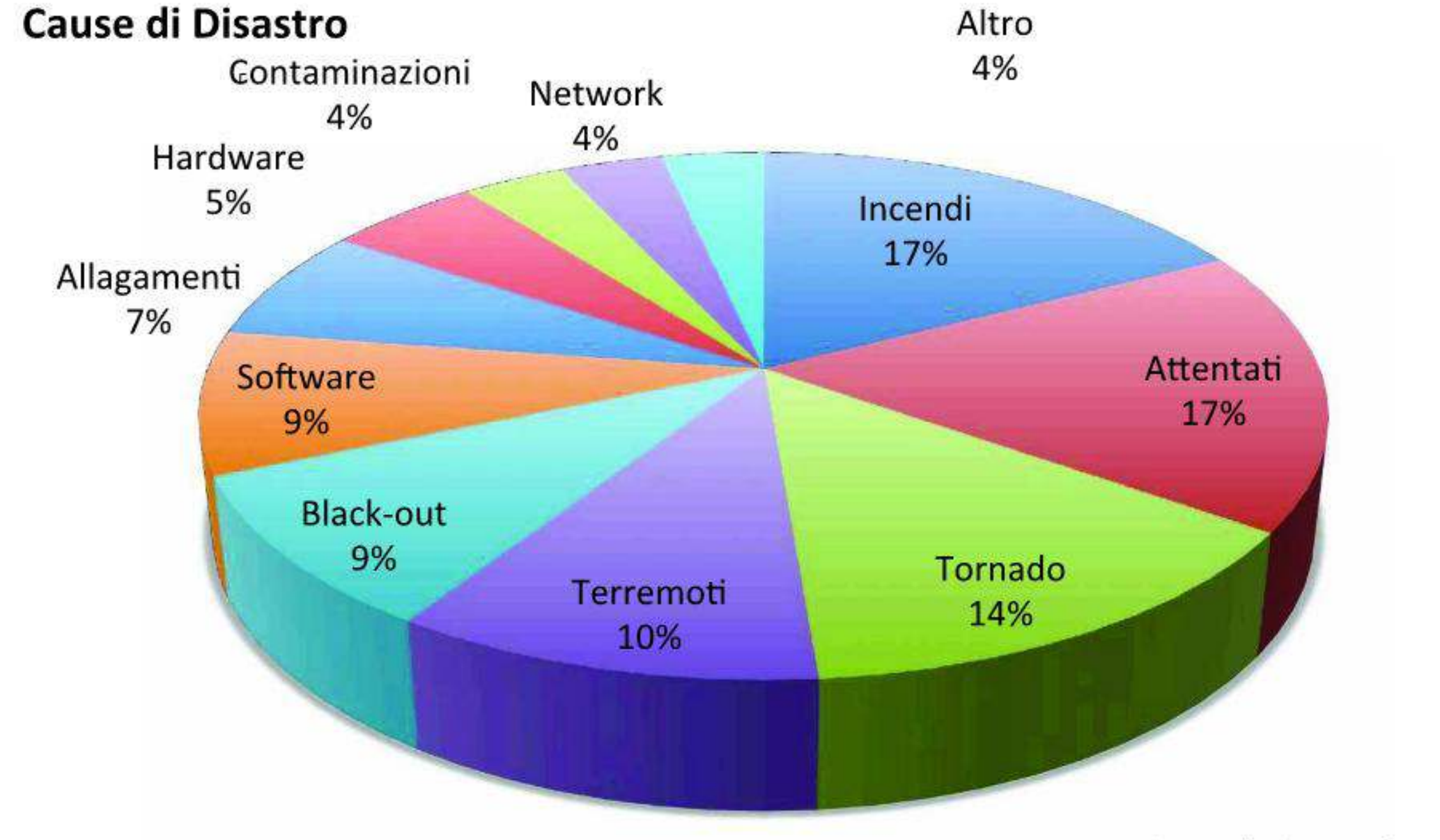
IDENTIFICAZIONE DEI RISCHI

Obiettivo dell'analisi del rischio è acquisire visibilità e consapevolezza sul livello d'esposizione al rischio, per poi costruire una lista preliminare dell'insieme delle possibili contromisure da attuare.
Occorre quindi identificare cosa necessita di protezione.

Le Criticità dei Sistemi Informatici

TIPOLOGIA DI BENI	RISCHI E MINACCE DA CONSIDERARE
Hardware (terminali, postazioni di lavoro, stampanti, dischi, supporti di memorizzazione,linee di comunicazione, apparati di rete, ...)	Malfunzionamenti dovuti a guasti, a sabotaggi, a eventi naturali come i terremoti, gli incendi e gli allagamenti, a furti e intercettazioni.
Software (di base o applicativo)	• Errori di progettazione • Presenza di codice malizioso (virus, cavalli di Troia, bombe logiche, backdoor). • Attacchi tipo denial of service
Dati	Accessi non autorizzati, modifiche volute o accidentali.
Risorse umane	Minacce alla sicurezza e alla salute degli impiegati.
Documentazione (contratti, manuali)	Perdita di informazione per eventi naturali o errori umani.

Le Criticità dei Sistemi Informatici



Fonte: Contingency Planning Research Inc.

Le Criticità dei Sistemi Informatici

CAUSA DELL'EMERGENZA	% DELLE RISPOSTE CHE HANNO INDICATO QUESTA CAUSA
Perdita di capacità IT	**25%**
Perdita di telecomunicazioni	**23%**
Perdita di personale	20%
Pubblicità negativa	16%
Perdita di competenze	14%
Interruzione della supply chain	12%
Inondazioni, cicloni	10%
Danno alla salute/sicurezza degli impiegati	8%
Danno alla reputazione dell'azienda	8%
Proteste di gruppi di pressione	7%
Perdita del sito	6%
Incendi	5%
Conflitti militari	5%
Problemi ambientali	4%
Danno alla salute dei clienti	4%
Attacchi terroristici	1%

Risulta evidente come il ruolo che il sistema informatico è arrivato a ricoprire al giorno d'oggi l' abbia reso parte integrante di tutti i processi di infrastrutture pubbliche e private.

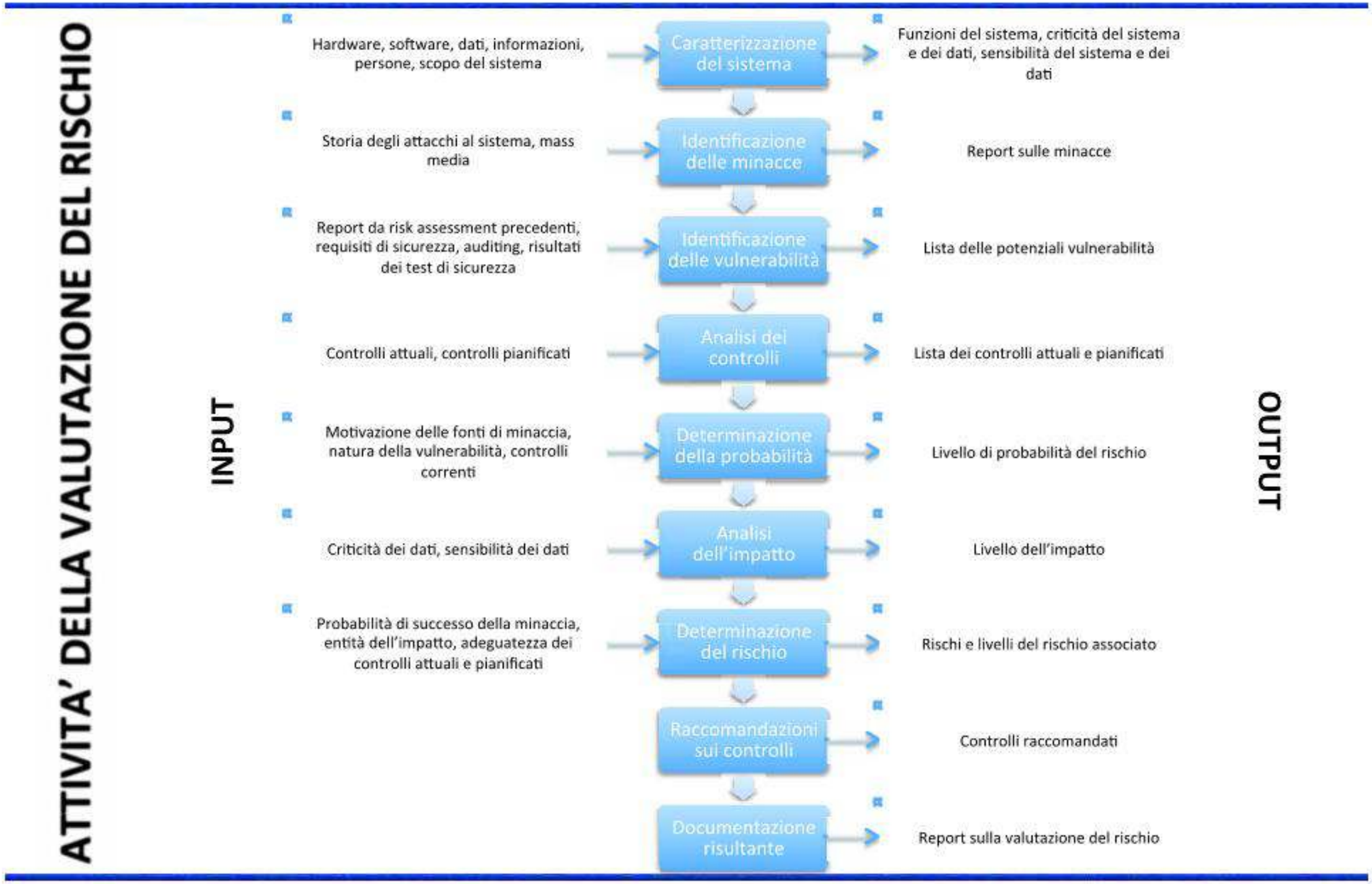
Questo però rende il sistema informatico la variabile di fallimento predominante delle attività quando non viene implementata una corretta strategia di gestione del rischio.

Nello schema che segue vediamo riassunti gli step delle varie attività relative alla valutazione del rischio.

A fronte di dati in ingresso reperiti da diverse fonti e con metodologie mirate vengono svolte delle attività per ottenere poi un risultato.

Tutti i risultati confluiranno poi in unico “Report della valutazione del rischio”.

Le Criticità dei Sistemi Informatici



CARATTERIZZAZIONE DEL SISTEMA

Per ottenere una valutazione dei rischi attendibili il primo step consiste nell'identificare gli scopi, i limiti e le caratteristiche del sistema analizzato:

- Hardware, Software, Interfacce, Sensibilità dei dati…
- Utenti del sistema, Architettura di sicurezza, Topologia della rete, Flusso delle informazioni…

Per ottenere queste informazioni si può ricorrere a diverse metodologie:

- Questionari
- Colloqui sul posto
- Verifica di documentazioni
- Utilizzo di tool di scansione automatizzati

IDENTIFICAZIONE DELLE MINACCE

FONTE DELLA MINACCIA	MOTIVAZIONE	AZIONI DELLA MINACCIA
Hacker, Cracker	Sfida Ego Ribellione	• Cracking • Social Engineering • Accesso non autorizzato al sistema
Criminale Informatico	Distruzione delle informazioni Divulgazione illegale di informazioni Guadagno economico Alterazione non autorizzata dei dati	• Crimine informatico • Corruzione delle informazioni • Falsificazione dell'identità • Intrusione nel sistema
Terrorista	Blackmail Distruzione Sfruttamento Vendetta	• Attacco terroristico • Attacco al sistema • Penetrazione del sistema • Manomissione del sistema
Spionaggio Industriale	Vantaggio competitivo Spionaggio economico	• Sfruttamento economico • Furto di informazioni sensibili • Social engineering • Accesso non autorizzato al sistema
Interni (impiegati poco formati, scontenti, negligenti, disonesti o licenziati)	Curiosità Ego Guadagno economico Vendetta Errori od omissioni non intenzionali	• Sabotaggio del sistema • Intrusione nel sistema • Inserimento di dati falsi o corrotti • Codice malizioso (virus, trojan, ...) • Blackmail

IDENTIFICAZIONE DELLE VULNERABILITA'

Lo scopo è di stilare una lista delle possibili vulnerabilità che potrebbero essere sfruttate dalle fonti di possibili minacce.

VULNERABILITA'	FONTE DELLA MINACCIA	AZIONE DELLA MINACCIA
Le credenziali di accesso di un impiegato licenziato non sono state rimosse dal sistema	Impiegati licenziati	Connettersi alla rete dell'azienda ed accedere a dati proprietari
Il firewall consente connessioni in ingresso sulla porta relativa al servizio *telnet* (porta 23) e l'utente *ospite* è abilitato sul server dell'azienda	Utenti non autorizzati (crackers, criminali, impiegati licenziati)	Utilizzare telnet per accedere al server dell'azienda e leggere i file di sistema con l'utente ospite
Il produttore ha identificato falle di sicurezza nel sistema ma le nuove patch non sono state ancora installate	Utenti non autorizzati	Ottenere accesso non autorizzato a file sensibili sfruttando vulnerabilità note del sistema
Il data center utilizza estintori a pioggia per spegnere eventuali incendi; non sono stati disposti teloni per proteggere l'hardware dall'acqua	Incendi, personale negligente	Esintori a pioggia attivati nel data center

ANALISI DEI CONTROLLI

Lo scopo di questo step è di verificare i controlli che sono stati implementati o pianificati per minimizzare o eliminare la possibilità (o la probabilità) che una minaccia faccia leva su una vulnerabilità del sistema.

Vengono effettuati controlli tecnici (software controllo accessi, metodi di criptazione, …) e non tecnici (verifiche sulle procedure operative, sicurezza ambientale, …)

DETERMINAZIONE DELLA PROBABILITA'

E' importante classificare le probabilità che una potenziale vulnerabilità possa essere sfruttata.

Ad esempio risulterà inutile implementare protezioni eccessive laddove è impossibile o altamente improbabile che quella determinata minaccia si concretizzi.

ANALISI DELL'IMPATTO

Il prossimo importante passo consiste nel misurare il livello di rischio per determinare l'impatto che potrebbe avere sul sistema una sua eventuale riuscita nello sfruttare una vulnerabilità.

I risultati potrebbero portare a:

- Perdita di integrità (corruzione dei dati)
- Perdita di disponibilità (sistema non più operativo)
- Perdita di confidenzialità (accesso a dati sensibili)

DETERMINAZIONE DEL RISCHIO

Per misurare il rischio può essere utile implementare uno schema d'aiuto che definisca il livello di pericolosità assegnando ad esempio un valore numerico all'impatto e alla probabilità della minaccia e mettendoli in relazione in una matrice:

PROBABILITA' DELLA MINACCIA	IMPATTO		
	Basso (10)	**Medio (50)**	**Alto (100)**
Alta (1.0)	Basso 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Media (0.5)	Basso 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Bassa (0.1)	Basso 10 x 0.1 = 1	Basso 50 x 0.1 = 5	Basso 100 x 0.1 = 10

Scala del rischio: Alto (da >50 a 100); Medio (da >10 a 50); Basso (da 1 a 10)

RACCOMANDAZIONI SUI CONTROLLI

Durante questa fase vengono consigliati i controlli da implementare per mitigare o eliminare i rischi identificati.

Lo scopo dei controlli raccomandati è ovviamente di ridurre a livelli accettabili il livello di rischio al sistema informatico e ai dati che contiene.

DOCUMENTAZIONE RISULTANTE (REPORT)

Completato il processo di risk assessment i risultati vengono riportati in un report ufficiale stilato in modo analitico e sistematico, per aiutare gli amministratori del sistema ad allocare le necessarie risorse per correggere le potenziali vulnerabilità.

MITIGAZIONE DEL RISCHIO

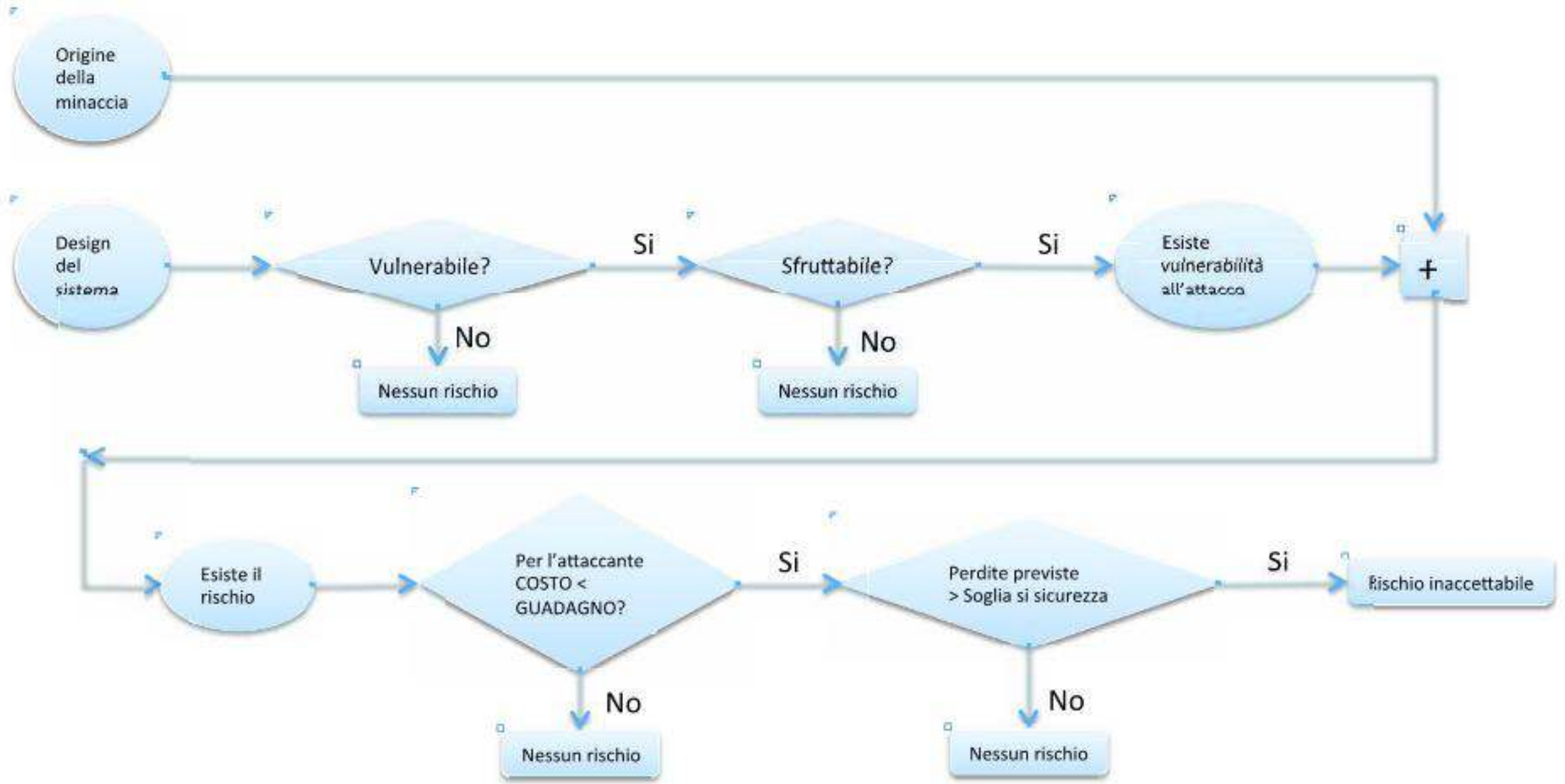
Il secondo processo della gestione del rischio consiste nel gestire le priorità, valutare ed implementare gli appropriati controlli di riduzione del rischio scaturiti dalla fase precedente.

OPZIONI DI MITIGAZIONE DEL RISCHIO

- **Assunzione del rischio**: accettare il rischio potenziale e continuare a gestire il sistema implementando controlli atti a ridurre il rischio ad un livello accettabile
- **Evitabilità del rischio**: evitare il rischio eliminando la causa e/o le conseguenze
- **Limitazione del rischio**: limitare il rischio implementando controlli che minimizzino l'impatto dello sfruttamento di una vulnerabilità da parte di una minaccia
- **Pianificazione del rischio:** gestire il rischio sviluppando un piano di mitigazione che dia priorità, implementi e gestisca i controlli
- **Ricerca e riconoscimento:** ridurre il rischio di perdite riconoscendo le falle e ricercando metodi per ridurre la vulnerabilità
- **Trasferimento del rischio:** trasferire il rischio utilizzando altre opzioni per compensare la perdita (es.: stipula di assicurazioni)

STRATEGIA DI MITIGAZIONE DEL RISCHIO

Per rispondere a domande come: "Quando devo intraprendere questa azione?" o "Quando devo implementare questi controlli per mitigare il rischio e proteggere il sistema?" può essere utile stilare un diagramma come questo:

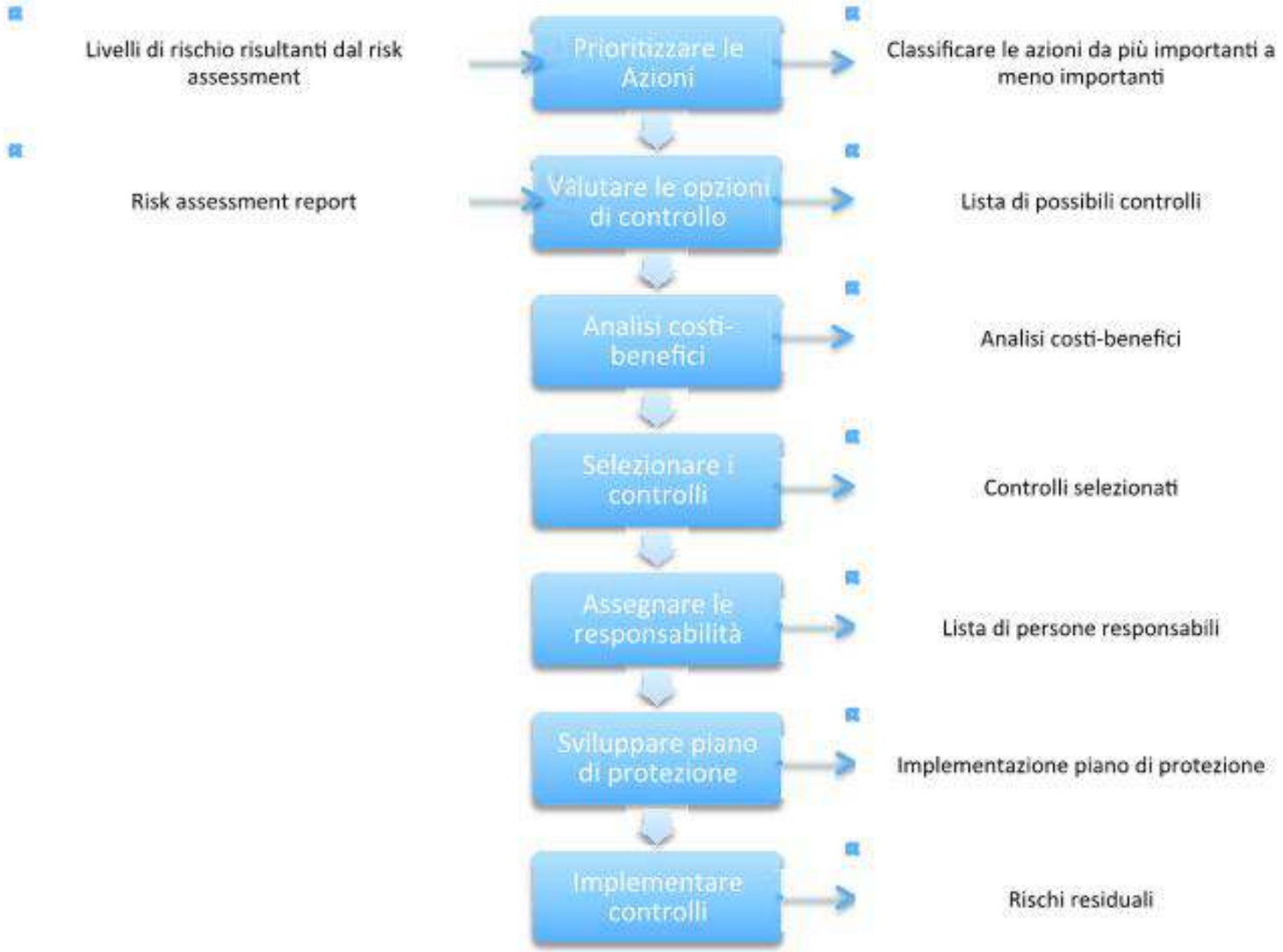


Nello schema che segue vediamo riassunti gli step delle varie attività relative alla mitigazione del rischio.

Anche in questo caso vengono raccolti dei dati in ingresso reperiti da diverse fonti e con metodologie mirate, vengono svolte delle attività per ottenere poi un risultato.

Al termine del processo avremo i controlli da attuare per mitigare il rischio.

ATTIVITA' DELLA MITIGAZIONE DEL RISCHIO



TIPOLOGIE DI CONTROLLI

Nell'implementare i controlli per mitigare il rischio un'organizzazione dovrebbe considerare aspetti tecnici, gestionali e di sicurezza delle operazioni che possano prevenire o limitare i danni in caso di minaccia.

CONTROLLI DI SICUREZZA TECNICA

Questi controlli possono spaziare da semplici a complessi e coinvolgono l'architettura del sistema.
Hardware, software, appliance e pacchetti di sicurezza: tutte queste misure dovrebbero lavorare insieme per proteggere i dati critici e sensibili.

Possiamo raggruppare i controlli tecnici in tre grandi categorie:

- Controlli tecnici di supporto
- Controlli tecnici preventivi
- Controlli tecnici di Individuazione e risoluzione

CONTROLLI TECNICI DI SUPPORTO

Sono per loro stessa natura pervasivi e correlati con molti altri controlli.

- **Identificazione**: consente di identificare utenti, processi e risorse di informazione in maniera univoca.
- **Gestione delle chiavi crittografiche**: le chiavi crittografiche devono essere gestite in modo sicuro quando funzioni di crittografia sono implementati in vari altri controlli.
- **Gestione della sicurezza**: Le funzionalità di sicurezza di un sistema IT possono essere incluse nel sistema operativo e aggiuntive e devono incontrare le necessità del sistema in caso di cambiamenti.
- **Protezioni di sistema**: come la separazione dei processi, l'assegnazione di permessi sui file limitati al ruolo e all'ambito dell'utente.

CONTROLLI TECNICI PREVENTIVI

Hanno lo scopo di inibire i tentativi di violare le policy di sicurezza.

- **Autenticazione**: metodi che consentono di verificare l'identità di un soggetto (password, PIN, smart card, certificati digitali, …)
- **Autorizzazione**: determinare chi può fare cosa all'interno del sistema
- **Controllo accessi**: rafforzare l'integrità e la confidenzialità dei dati con sistemi di controllo accessi (profili utente, ruoli, ACL, …)
- **Comunicazioni protette**: in un sistema informatico un alto livello di sicurezza è strettamente collegato all'attendibilità delle comunicazioni. Metodi protetti di comunicare (VPN, IPSEC, DES, 3DES, …) consentono di minimizzare gli attacchi
- **Privacy delle transazioni**: enti governativi e privati stanno sempre più aumentando i controlli per garantire la privacy delle transazioni (SSL, secure shell, …)

CONTROLLI TECNICI DI INDIVIDUAZIONE E RISOLUZIONE

I controlli di individuazione avvisano in caso di violazioni delle policy di sicurezza; i controlli di risoluzione consentono di ripristinare le funzionalità del sistema compromesse.

- **Audit**: la revisione di eventi rilevanti ed il monitoraggio delle anormalità del sistema sono elementi chiave per il ripristino in caso di minaccia
- **Intrusion detection**: è essenziale individuare brecce alla sicurezza in modo da poter agire il più in fretta possibile
- **Prova di integrità**: analizza l'integrità del sistema e ne identifica le irregolarità e le potenziali minacce
- **Ripristino di stato di sicurezza**: consente ad un sistema di ritornare ad uno stato precedente e sicuro dopo che che c'è stata una breccia alla sicurezza
- **Individuazione e rimozione virus**: ovviamente è necessario che server e workstation abbiano antivirus installati ed aggiornati.

GRAZIE