Il Security e risk management delle infrastrutture

Un approccio epistemiologico e metodologico

Lombardi dott. Andrea

- Ha prestato servizio presso la compagnia Genio Pionieri della Brigata paracadutisti Folgore, da li è transitato alla Scuola Sottufficiali di Viterbo, dove è stato selezionato per il 9° Reggimento d'assalto col Moschin, congedandosi nel 1997 come Maresciallo incursore.
- Negli anni 2000 ha partecipato a vari progetti di sminamento umanitario in Afghanistan e Iraq, ricoprendo l'incarico di De-mining technical advisor.
- Dal 2003 al 2005 è stato richiamato in servizio e ha partecipato alla costituzione delle Unità Cinofile dell'Esercito Italiano.
- Attualmente presta servizio con l'European External Action Service come Regional Security Officer per la Turchia e il Turkmenistan.
- Ha conseguito una laurea breve in Scienze per l'investigazione e per la sicurezza, presso l'università di Perugia, Un Master in Science in Security e risk management, presso l'università di Leicester, in UK e un Master di II livello, in Criminologia e Cybersecurity presso la Fondazione INUIT di Tor Vergata.

Qualche definizione

- **Management:** è un'arte che coordina gli sforzi delle persone per raggiungere traguardi e obiettivi utilizzando le risorse disponibili in modo efficiente ed efficace. Comprende la pianificazione, l'organizzazione, l'assunzione di personale, la guida o la direzione e il controllo di un'organizzazione per raggiungere l'obiettivo. Le risorse comprendono la distribuzione e la manipolazione di risorse umane, risorse finanziarie, risorse tecnologiche e risorse naturali.
- **Security:** L'insieme delle strategie adottate per proteggere un infrastruttura/ organizzazione.
- **Security e risk management:** è tutta quella serie di attività che in maniera scientifica mirano a mitigare il rischio.
- **Infrastruttura:** il complesso degli impianti e delle installazioni occorrenti all'espletamento di servizi.
- **Rischio:** l'eventualità di subire un danno, la potenzialità che un qualcosa porti ad un evento indesiderato.
  - Diretto.
  - Indiretto.

  I rischio può anche essere definito come il prodotto tra la probabilità che un evento accada e le sue conseguenze e cioè. R = P *C.

Lo scopo della sicurezza

➢Essa mira a:

- **Deter** - Fungere da deterrente
- **Detect** - Identificare i rischi in anticipo.
- **Delay** – Ritardare l'attacco
- **Defend** - Proteggere il proprio obiettivo.

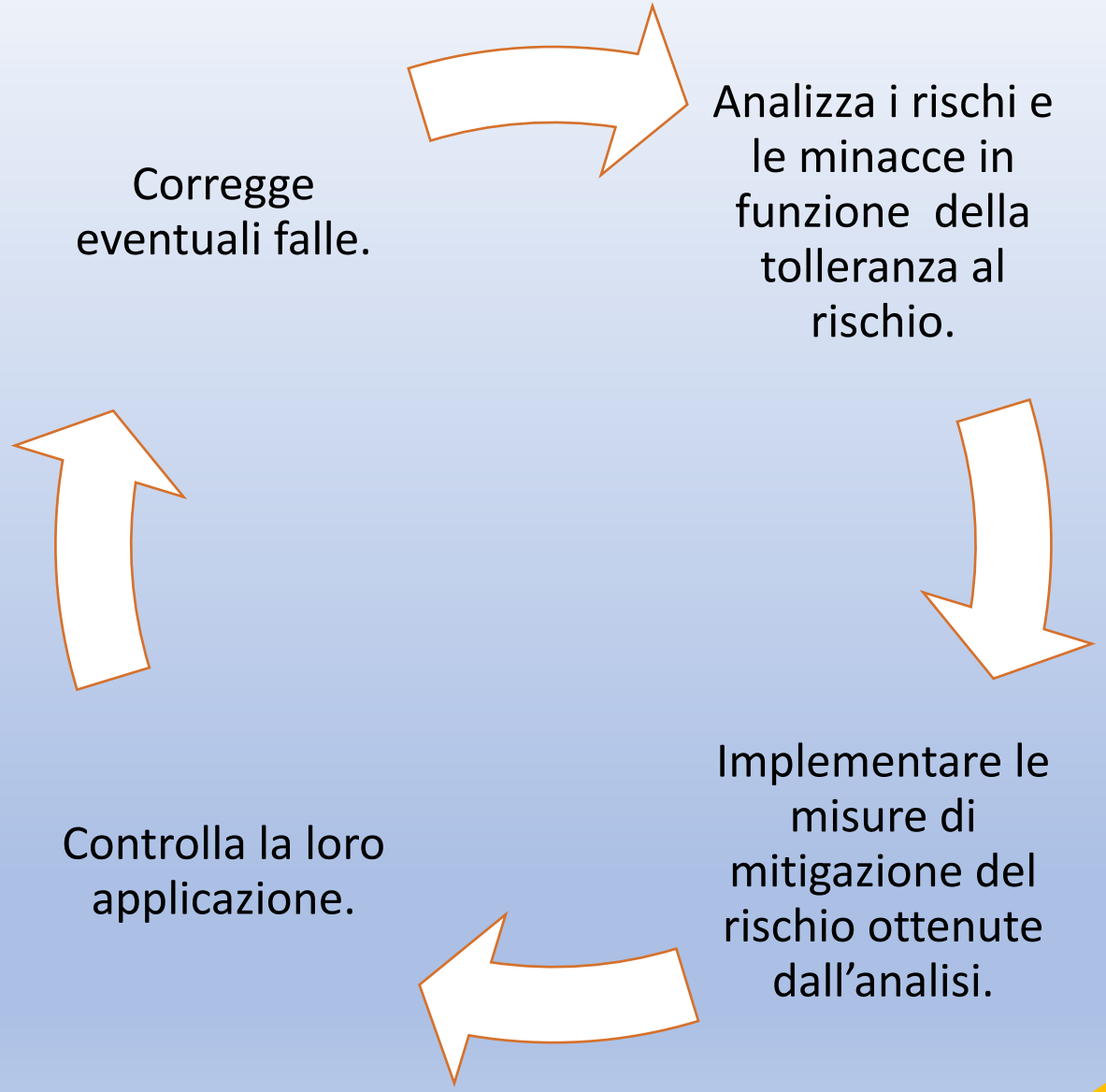
In pratica

La sicurezza usa le informazioni, lo spazio, le barriere e le procedure. Allo scopo di garantire le 4 D.

Il security and risk management mira a far si che il tempo necessario per sviluppare un evento pericoloso per un infrastruttura/ organizzazione (Te) sia maggiore del tempo di allarme (Ta) e del tempo necessario di intervento (Ti) per l'infrastruttura/ organizzazione.

$Te > Ta + Ti$

Il ciclo di security e risk management in pratica



Quali informazioni sono necessarie per il risk management

➢ Informazioni sui rischi presenti nell'area geografica dove l'infrastruttura è posta:

- I rischi generati da fattori umani.
- i rischi generati da eventi naturali.

➢ Informazioni riguardanti l'infrastruttura:

- Tipo di infrastruttura.
- Dove è locata.
- Tipi di allacciamenti alla rete (energetica idrica, fognaria, internet ecc.).
- Tipo di costruzione (materiali utilizzati, test strutturali eseguiti e certificazioni ottenute, planimetria, cablaggi ecc.).
- Accessi all'infrastruttura (dove sono locati e tipologia).
- Se ci sono altri utilizzatori dell'infrastruttura e chi sono.
- Servizio di sicurezza e opere di sicurezza già esistenti.

L’analisi delle informazioni in funzione della gestione dei rischi

➢Due modelli (adattati) provenienti dal mondo finanziario:

- La PEST (EL) analisi.
- La SWOT analisi.

Analisi PEST (Politica, Economica, Sociale e Tecnica) adattata

Tipo di rischio	Politica	Economica	Sociale	Tecnica	Tipo di rischio		Probabilità	Conseguenze
					Diretta	Indiretta		
Terrorismo								
Crimine								
Conflitti Armati								
Violenza Politica								
Spionaggio								
Calamità Naturali								
Altro								

Un esempio

Tipo di rischio	Politica	Economica	Sociale	Tecnica	Tipo di minaccia		Probabilità	Conseguenze
					Diretta	Indiretta		
Terrorismo	Nel paese opera il gruppo terroristico di estrema destra denominato Aquile Bianche. Il gruppo si oppone al governo.	Il gruppo sembra ricevere sovvenzioni da paesi confinanti.	Il gruppo riceve un limitato supporto al supporto dal gruppo etnico dei Bardoli.	Il gruppo agisce maggiormente tramite attentati di tipo dinamitardo contro infrastrutture e mezzi governativi. Non sono mai state attaccate aziende sia nazionali che internazionali.		X	Trascurabile	Moderate
Crimine	Il paese è afflitto da una criminalità organizzata molto vasta. I gruppi operanti fanno capo a 3 grosse famiglie: gli Hakka, gli Xizie, e li Ypsilo.	Le entrate di questi gruppi arrivano maggiormente con il traffico della droga e il commercio di armi. Ma non sono di meno le rapine e i furti	La corruzione nel paese è molto alta, anche all'interno delle forze di Polizia e il sistema giudiziario	Traffico di droga, commercio illegale di armi, rapine e furti.	X		Moderate	Moderate
Calamità naturali	Il paese è soventemente affetto da eventi sismici anche di grossa intensità	I danni arrecati alle costruzioni e alle infrastrutture sono spesso seri.	Anche se nel paese esiste una legge sull'edilizia antisismica le certificazioni della stessa non sono affidabili dovuto alla corruzione dilagante.	Terremoti di scala richter fino a 6.5	x		Moderate	Maggiori

Analisi SWOT (Punti di Forza, Punti di debolezza, Correzioni richieste e Rischi/Minacce) adattata.

Oggetto Analizzato	
Punti di forza	Punti di debolezza
Opportunità	Rischi/minacce
Probabilità	Conseguenze

Un esempio

Sistemi antincendio dell'infrastruttura	
Punti di forza	Debolezze
L'intera infrastruttura è provvista sia di sistemi di rivelazione di fumo che di spegnimento automatico degli incendi. La struttura è provvista di un adeguato numero di uscite di emergenza. Segnali e luci di emergenza sono ben collocati I punti di raccolta sono ben definiti e segnalati.	La struttura ha molte parti in legno e infiammabili. La manutenzione dei dispositivi antincendio non viene effettuata da personale qualificato. Gli estintori dell'infrastruttura sono solo di classe A e la manutenzione è dubbia e questi non posizionati correttamente. Le vie di fuga dalla struttura sono spesso ostruite da materiale di deposito, come attrezzi per la pulizia e vecchi mobili. La stanza server, essendo stata aggiunta in un secondo tempo, non ha installato un adeguato sistema di rilevazione del fumo e del calore e altresì antincendio. L'addestramento all'evacuazione dell'edificio non viene effettuato da lungo tempo. I piani di emergenza non sono aggiornati
Opportunità	Minacce
Rivedere i contratti di manutenzione del sistemi di rilevazione e spegnimento incendi. Sensibilizzare il personale di pulizia a non utilizzare le vie di fuga dall'infrastruttura come rispostigli. Condurre l'addestramento all'evacuazione dell'infrastruttura il prima possibile. Aggiornare i piani di emergenza	I sistemi automatici di rivelazione del fumo potrebbero non funzionare Le vie di fuga in caso di evacuazione dell'infrastruttura potrebbero risultare ostruite e di on facile percorrenza.
Probabilità	Conseguenze /Vulnerabilità
Alta	Maggiori/Critiche

Calcolare le Vulnerabilità

- Analizzate le informazioni con i moduli che abbiamo visto sopra dovremmo identificare le Vulnerabilità, dell'infrastruttura/ organizzazione tramite un processo deduttivo.
  - Per far ciò si dovranno considerare i punti di forza, i punti deboli e la resilienza dell'infrastruttura/organizzazione.
- Alla fine del processo essa potrà essere; Critica (5), Alta (4), Media (3), Bassa (2), Trascurabile (1).

Calcolare le probabilità

- Le probabilità si basano sulla possibilità che un evento possa accadere.
  - Possono essere calcolate con la formula Probabilità (P) = Minaccia (M) x Vulnerabilità (V).
- Al termine della stima la probabilità potrà essere: Molto Alta (5), Alta, Media (3), Bassa (2), Remota (1).

Calcolare la minaccia

➢L’identificazione della Minaccia è un processo di Brainstorming e si basa sull’analisi dei seguenti parametri:

- Lo storico della minaccia.
- Il contesto (fattori inibenti).
- Le potenzialità della minaccia.
- L’intento.

➢Alla fine del processo di brainstorming essa potrà essere: Critica (5), Alta (4), Media (3), Bassa (2), Trascurabile (1).

Calcolare le conseguenze

➢Il calcolo delle conseguenze tiene conto dei seguenti parametri:

- I danni arrecati a persone.
- I danni fisici arrecati alle strutture e i conseguenti danni di tipo economico.
- Il tempo necessario per ripristinare l'operatività e le funzioni dell'infrastruttura.
- Le eventuali ricadute di tipo reputazionale.

➢Anch'esso si ottiene tramite un processo di brainstorming che identifica le conseguenze come: Critiche (5), Maggiori (4), Moderate (3), Minori, Trascurabili (1) .

La matrice del rischio – R = P x C.

Probabilità	Conseguenze				
	Trascurabili (1)	Minori (2)	Moderate (3)	Maggiori (4)	Critiche (5)
Molto alta (5)	Media (5)	Alta (10)	Alta (15)	Critica (20)	Critica (25)
Alta (4)	Media (4)	Media (8)	Alta (12)	Alta (16)	Critica (20)
Moderata (3)	Bassa (3)	Media (6)	Media (9)	Alta (12)	Alta (15)
Bassa (2)	Bassa (2)	Media (4)	Media (6)	Media (8)	Alta (10)
Remota (1)	Bassa (1)	Bassa (2)	Bassa (3)	Media (4)	Media (5)

Calcolare L’impatto

- L’Impatto (I) = alla capacità di Resilienza dell’infrastruttura/organizzazione (D) x le Conseguenze (C). I = D x C.
- L’impatto che un evento dannoso possa accadere per la nostra infrastruttura potrà essere (nel rispetto della tavola vista sopra potrà) Critico, Alto, Medio, Basso.

Calcolare la capacità di Resilienza dell'infrastruttura/ organizzazione

- L'identificazione della capacità di Resilienza è un processo deduttivo che dovrà considerare l'intero delle misure di mitigazione del rischio messe in opera come:
  - Barriere
  - Illuminazione
  - Sistemi CCTV
  - Sistemi di allarme
  - Guardi di sicurezza
  - Altro.
- Alla fine del processo di brainstorming la capacità di Resilienza potrà essere Inesistente (5), Debole (4), Parziale (3), Forte (2), Completa (1).

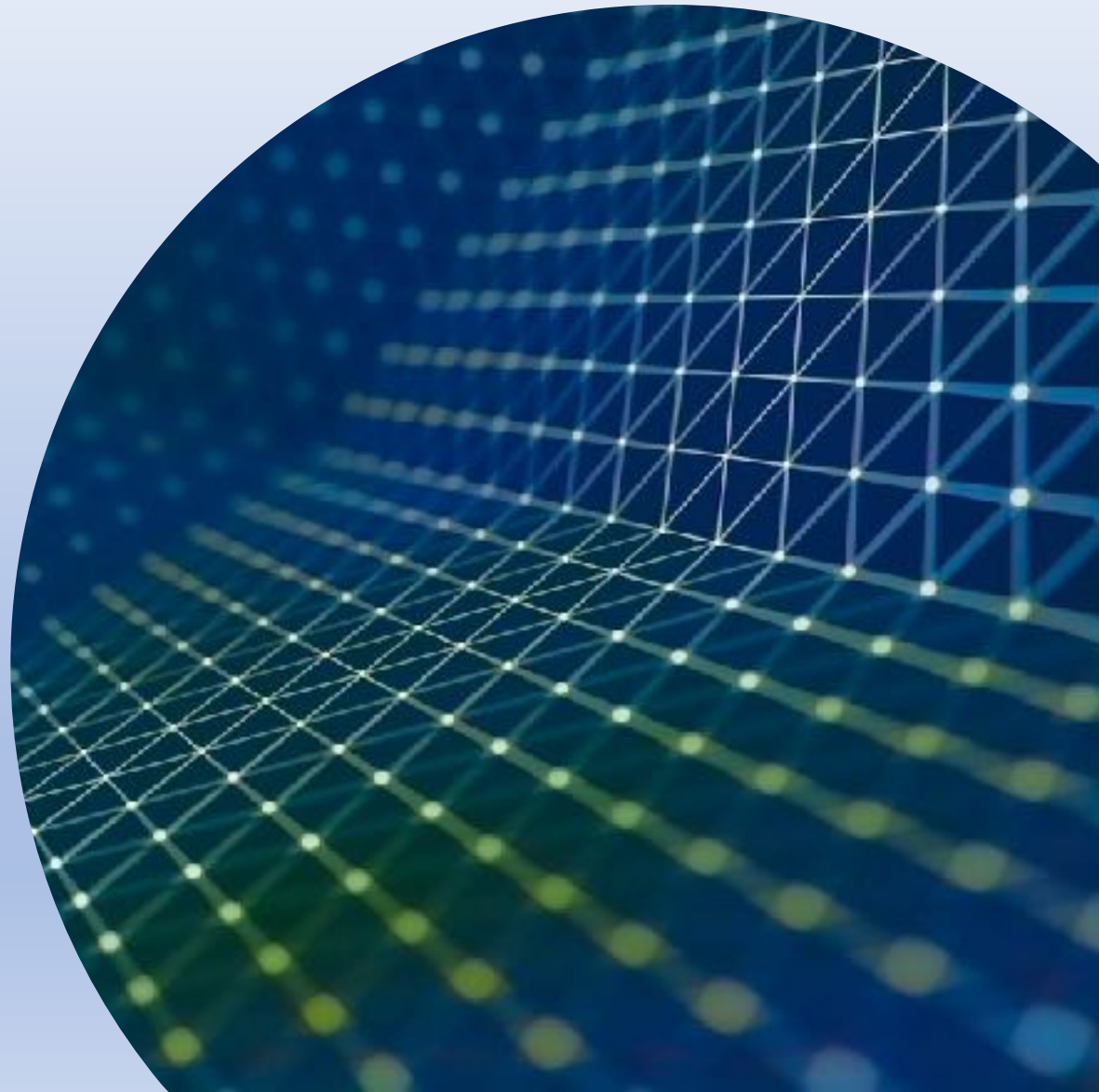
Come affrontare il rischio

EVITARE IL RISCHIO.

MITIGARE IL RISCHIO.

ACCETTARE IL RISCHIO.

TRASFERIRE IL RISCHIO.



Caso Studio - Scenario

La nostra infrastruttura è attenzionata da elementi di intelligence avversa e non è provvista di nessun locale per la custodia di documenti classificati. Ciò nonostante ci viene richiesto di tenere nell'infrastruttura alcuni documenti classificati (livello dei documenti da conservare CONFIDENZIALE, conseguenze in caso di furto MODERATE = 3).

Caso Studio – Analisi Vulnerabilità

- Decidiamo di custodire i documenti all'interno di un cassetto nell'ufficio sicurezza (livello di Vulnerabilità della resistenza della serratura del cassetto ALTA = 4).
- La porta dell'ufficio di sicurezza è una porta antifurto con simile serratura (livello di Vulnerabilità della porta dell'ufficio BASSA = 2).

Caso Studio – Analisi Minacce

- Le guardie sono assunte localmente e la Minaccia che possono essere attenzionate dall'intelligence avversa è alta (probabilità che le guardie possano tentare il furto ALTA = 4).
- All'interno dell'ufficio sicurezza, oltre a Noi, ha accesso l'assistente alla sicurezza, assunto localmente, ex ufficiale del passato regime, critico con il governo corrente (Minaccia che tenti il furto MEDIA = 3).
- Oltre a Noi e all'assistente alla sicurezza nell'ufficio ha anche accesso il personale di pulizia, che però accede all'ufficio solo in presenza del titolare (Minaccia che tenti il furto REMOTA = 1).
- No si valuta possibile che il furto dei documenti classificati possa essere tentato da elementi esterni all'infrastruttura.

Caso Studio – Analisi Minacce + Vulnerabilità

➢ **Minacce**

- Minaccia 1 – Guardie = ALTA (4).
- Minaccia 2 – Assistente Sicurezza = MEDIA (3).
- Minaccia 3 – Personale di Pulizia = REMOTA (1).

➢**Vulnerabilità**

- Vulnerabilità 1 – Cassetto Interno Ufficio Sicurezza = ALTA (4).
- Vulnerabilità 2 – Porta Ufficio Esterna Ufficio Sicurezza = BASSA (2).

Caso Studio – Analisi della Probabilità

- P1 = Guardie all’entrata (Minaccia = 4) x Rottura sigillo busta copia chiavi ufficio sicurezza (Vulnerabilità = 2) = 8 MEDIA.
- P2 = Assistente Sicurezza (Minaccia = 3) x Cassetto Interno Ufficio (Vulnerabilità = 4) = 12 ALTA.
- P3 = Personale di pulizia (Minaccia = 1) x Cassetto Interno Ufficio (Vulnerabilità = 4) = 4 MEDIA.
- Il calcolo del Rischio sarà R = P (Agg di P/N) x C.

La pianificazione dei lavori per la mitigazione del il rischio.

Tipo di rischio	Possibile scenario	Probabilità/ Conseguenze		Misure in atto	Misure correttive richieste	Urgenza	Costo	Incaricato	Da finalizzare entro	Eseguito

Piani essenziali per la gestione giornaliera e di emergenza di un infrastruttura.

➢ Procedure giornaliere:

- Procedure di accesso all’infrastruttura.
- Procedure di ricezione di posta, pacchi, fornitori, ecc.
- Procedure di accesso alle aree sensibili.
- Altre procedure necessarie per l’operatività dell’infrastruttura.

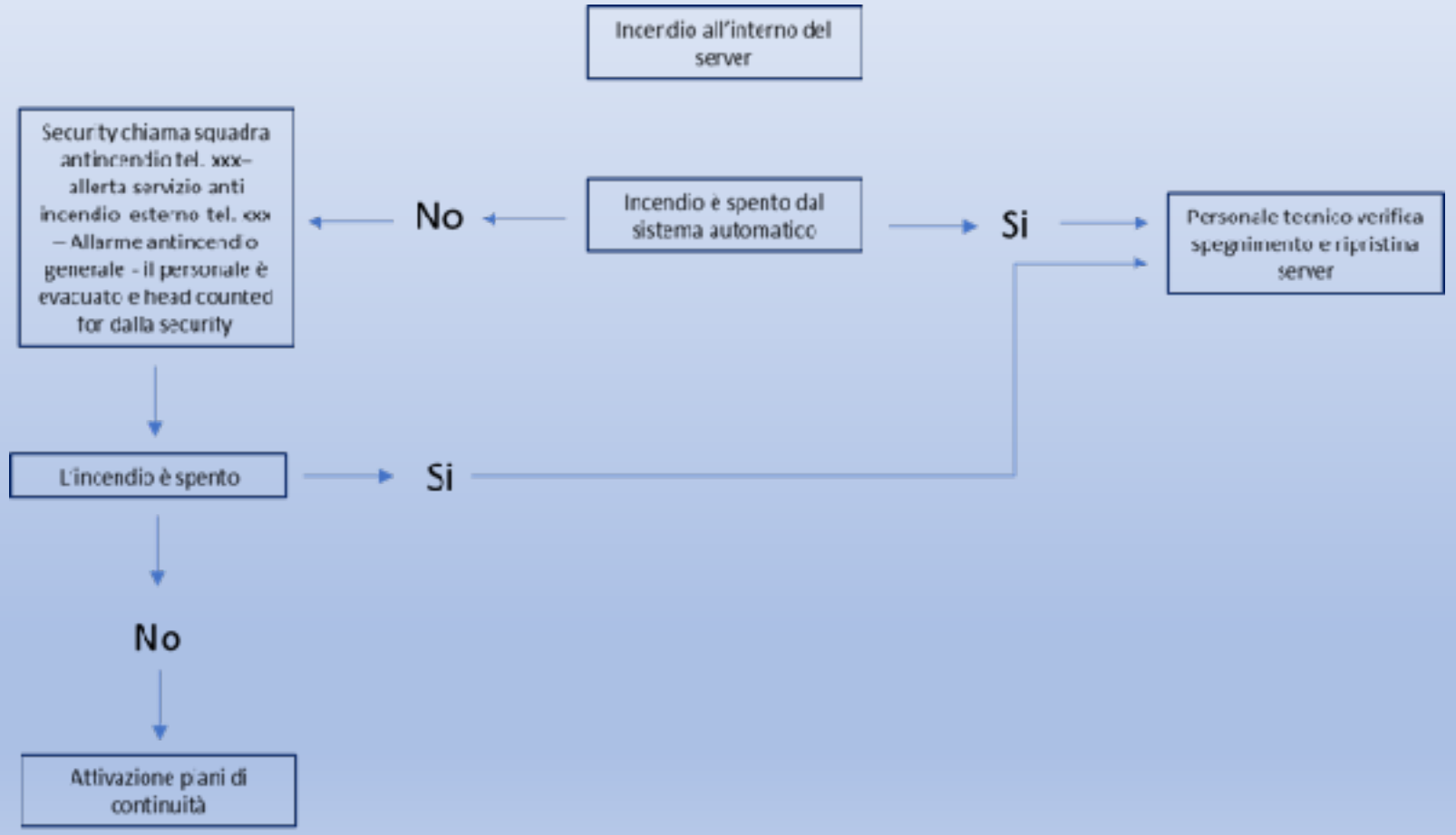
➢ Piani di contingenza:

- Piani di evacuazione parziale o totale dell’infrastruttura in caso di emergenza.
- Piani di continuità durante e dopo un’emergenza.
- Piani antincendio e in caso di altri possibili disastri a seconda di dove l’infrastruttura si trova e delle sue attività
- Piani per fronteggiare emergenze mediche.
- Piani per la comunicazione con i media in caso di emergenze dell’infrastruttura.
- Atri piani a seconda della necessità.

Una procedura o un piano di emergenza deve

- Essere scritta in maniera dettagliata ma sintetica.
- Essere messe a conoscenza di tutta l’organizzazione.
- Essere esercitata con periodicità.
- Essere verificata e aggiornata.

Un esempio di piano di contingenza



Domande?