La protezione delle infrastrutture critiche: approccio multidisciplinare per la valutazione del rischio sicurezza anti-sabotaggio/anti-terrorismo

Autori:

Dott. ing. Claudio Todaro
(esperto in Security Risk Management & Intelligence Analysis)

Ten. Col. Vincenzo Iavarone
(esperto in Security per le Infrastrutture Critiche & Crisis Management in scenari non convenzionali)

La recente entrata in vigore del D.Lgs. 61 dell'11 aprile 2011 come recepimento in Italia della Direttiva Europea 2008/114/CE riguardante la Protezione delle Infrastrutture Critiche Europee ha aperto il dibattito sulla corretta metodologia per la redazione (e la successiva gestione) del Piano Sicurezza dell'Operatore come elemento fondamentale del Security Management.
Il testo del citato decreto prevede all'art. 12 l'obbligo di tale piano a cura del soggetto responsabile dell'infrastruttura e nell'appendice B ne definisce le linee guida, basate su una metodologia di Risk Analysis.
Senza limitarsi al campo di applicazione definito dal citato decreto (le "ICE", Infrastrutture Critiche Europee), bensì considerando le "infrastrutture critiche" in generale, viene qui presentato un approccio multidisciplinare per un'esaustiva valutazione del rischio sicurezza (focalizzato ad aspetti anti-sabotaggio/anti-terrorismo) e per un'efficace stesura del Piano di Sicurezza.
Tale approccio considera diverse discipline cooperanti: l'analisi del rischio (secondo la norma internazionale ISO 31000:2009), l'analisi di scenario (basata essenzialmente su informazioni di Intelligence, per un'attenta definizione delle minacce presenti nel contesto di interesse per l'infrastruttura), il "Technology Scouting & Design" (per una scelta ottimizzata delle piattaforme tecnologiche e per la relativa progettazione di sistema) ed il "Security System Design" (per un'efficace integrazione del "fattore umano" nella catena di Comando & Controllo).
La metodologia realizza pertanto una combinazione sinergica ed interdipendente dei tre elementi fondamentali (uomo, tecnologie, procedure) nel complesso sistema di protezione dell'infrastruttura critica da rischi derivanti da atti di sabotaggio e terrorismo, ponendosi come efficace e dinamico strumento di Security Governance.

1. Perché un "protocollo"?

La necessità di provvedere ad un'analisi esaustiva della Sicurezza Fisica di una Infrastruttura Critica[1] rende opportuno il ricorso ad uno strumento efficace di "valutazione guidata a 360°", ovvero secondo un approccio di tipo *all hazard*.
Ad oggi in Italia non esiste uno strumento standardizzato e condiviso per un'analisi dei rischi di sicurezza AS/AT (antisabotaggio/ antiterrorismo). Ciò è principalmente dovuto al fatto che tale "tematica", afferente al settore della Sicurezza Nazionale, è di competenza di diversi enti istituzionali (Forze dell'Ordine, Forze Armate, strutture di intelligence, ecc.), ciascuno dei quali provvede operativamente in modo autonomo e secondo le proprie peculiarità organizzative e di attribuzione.
Il D.Lgs. 61 dell'11 aprile 2011 (che recepisce in Italia la Direttiva Europea 2008/114/CE riguardante la Protezione delle Infrastrutture Critiche Europee[2]) ha introdotto l'obbligo per il gestore dell'Infrastruttura Critica (soggetto di carattere pubblico o privato) di redazione del "Piano Sicurezza dell'Operatore" (con riferimento all'art. 12 e all'appendice B del decreto). Appare pertanto chiaro che l'argomento della "protezione antisabotaggio/antiterrorismo" costituisce una parte fondamentale di tale piano e sul quale concorrono elementi di valutazione sino ad oggi di esclusiva competenza dei soggetti istituzionali preposti (secondo le vigenti disposizioni legislative).
Si è ritenuto pertanto utile predisporre uno specifico strumento di Risk Analysis[3], da rendere fruibile al *Security Manager* dell'Infrastruttura Critica in cooperazione con gli enti istituzionali competenti.
Tale strumento considera diversi settori disciplinari (analisi del rischio, analisi di scenario, definizione tecnologica, security management) e si rende pertanto necessario un approccio "di team", ove possano concorrere sinergicamente le diverse competenze professionali.
Per la definizione del "protocollo" è stata svolta altresì un'approfondita analisi di quanto esistente in materia in ambito internazionale (in particolare presso le competenti strutture delle Nazioni Unite e presso organismi di paesi dell'area NATO), individuando ed elaborando elementi applicabili efficacemente al nostro contesto nazionale.

2. Il Gruppo di Valutazione

Le attività di valutazione (condotte secondo il protocollo qui illustrato) richiedono la costituzione di un "team multidisciplinare", coordinato dal Responsabile del Gruppo di Valutazione (a sua volta designato dall'Operatore dell'Infrastruttura Critica ed in possesso delle necessarie prerogative di professionalità e di indipendenza di giudizio).
Il Responsabile del Gruppo di Valutazione può avvalersi, in relazione alla complessità dell'Infrastruttura Critica oggetto di valutazione, di uno o più specialisti in qualità di componenti del Gruppo di Valutazione stesso (esperti di tecnologie e di *security management*) che possano contribuire in modo efficace ed esauriente all'analisi dei rischi.
Il Responsabile del Gruppo di Valutazione si interfaccia con il Funzionario alla Sicurezza dell'Infrastruttura Critica (a sua volta "punto di contatto" con gli organismi competenti secondo quanto previsto dall'art. 12 comma 1 del D.Lgs.61/2011).
Le informazioni riguardanti l'analisi dei rischi devono essere gestite secondo l'art. 12 del citato decreto e l'intero Gruppo di Valutazione, in qualità di "prestatore d'opera" nei confronti dell'Operatore responsabile

[1] Si definisce "Infrastruttura Critica" un'infrastruttura, ubicata in uno stato membro dell'Unione europea, essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilita' di mantenere tali funzioni.
[2] Si definisce "Infrastruttura Critica Europea (ICE)" un'infrastruttura critica ubicata negli Stati membri dell'UE il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due stati membri.
[3] Per la "Risk Analysis" si fa riferimento alla norma internazionale ISO 31000:2009.

dell'Infrastruttura, deve essere considerato come parte integrante della struttura di sicurezza ivi operante. Pertanto i singoli componenti devono essere provvisti di apposito NOS (Nulla Osta di Segretezza) qualora le informazioni da trattare siano con classifica superiore a "Riservato".

3. La valutazione dei rischi

Il Gruppo di Valutazione provvede all'acquisizione e all'elaborazione dei dati necessari all'Operatore dell'Infrastruttura Critica per l'adozione delle decisioni finalizzate ad un'efficace "messa in sicurezza" dei propri *assets*.
Quest'attività, ad elevato livello di specializzazione, necessita di sei passaggi operativi che consentono l'elaborazione di una adeguata analisi e valutazione dei rischi:
- comprensione dell'organizzazione operante all'interno dell'Infrastruttura Critica e determinazione delle risorse a rischio;
- individuazione dei fattori di rischio e delle relative vulnerabilità;
- determinazione delle probabilità di accadimento dell'evento ostile e della relativa frequenza;
- previsione degli effetti che un evento ostile potrebbe provocare all'Infrastruttura Critica;
- studio delle possibili strategie difensive e degli eventuali impatti sull'operatività dell'Infrastruttura Critica;
- valutazione del rapporto costi/benefici nella strategia di protezione AS/AT applicabile al contesto.

Tale processo operativo viene attuato attraverso la metodologia illustrata in fig. 1, che prevede un'attività di valutazione iniziale, un'analisi di scenario della minaccia (supportata da un'accurata attività di Intelligence Analysis) e la definitiva implementazione delle necessarie azioni di mitigazione e contrasto sui punti di vulnerabilità rilevata.
Viene parallelamente analizzato un eventuale piano di attività per la "gestione della crisi", da attuarsi nel caso di una *escalation* degli eventi indesiderati (Crisis Management Plan) e che ha lo scopo di garantire adeguati livelli di *Business & Operations Continuity*. Ove tale piano sia mancante, il Gruppo di Valutazione fornisce i necessari elementi per la sua implementazione.
Successive attività di verifica e di riesame da parte del Gruppo di Valutazione assicurano l'efficacia di tutte le azioni introdotte dall'Operatore dell'Infrastruttura Critica, al fine di garantirne i più elevati standard di protezione fisica.

Il "Protocollo di Valutazione" è un documento strutturato in dieci capitoli.
I primi quattro capitoli sono introduttivi (secondo l'impostazione di una comune "norma"): scopo e campo di applicazione, ruoli e responsabilità, definizioni, riferimenti normativi e legislativi.
Nei successivi tre capitoli (quinto, sesto e settimo) viene condotta la cosiddetta "analisi di scenario".
Il quinto capitolo riguarda le attività di acquisizione e analisi delle informazioni generali del sito interessato (destinazione, georeferenziazione e morfologia dell'area).
Il sesto capitolo tratta le informazioni di dettaglio: planimetrie, informazioni di caratterere politico/sociologico riguardanti la popolazione circostante, principali eventi riscontrati nell'area circostante o su siti similari in altre aree, tipologia delle attività operate nel sito, tipologia e consistenza del personale operante nel sito, eventuali informative per minacce e/o eventi dolosi riguardanti il sito. Questa sezione del Protollo di Valutazione è particolarmente delicata, in quanto costituisce la cosidetta "analisi di intelligence" da condursi sulla base delle informazioni raccolte dagli organismi istituzionali preposti (con eventuale "classifica di segretezza") e che deve consentire un'attenta ed esauriente valutazione della minaccia.
Nel settimo capitolo vengono illustrate le modalità di conduzione del sopralluogo al sito da parte del Gruppo di Valutazione, fornendo i criteri di valutazione dei vari elementi: accesso, sorveglianza, protezione delle aree interne, protezione delle informazioni sensibili, protezione del personale, sistema di gestione della sicurezza. Gli elementi raccolti

consentono un'accurata valutazione della vulnerabilità del sito (valutazione qualitativa).
Nell'ottavo capitolo viene illustrata la metodologia per la cosiddetta "analisi dei rischi", con una valutazione quantitativa di impatto[4] e probabilità[5] per il singolo evento ostile.
La valutazione dell'impatto avviene secondo la seguente scala di valutazione (riportata in dettaglio nella fig. 2): trascurabile, minore, moderato, severo, critico.
La valutazione della probabilità avviene invece secondo la seguente scala di valutazione (riportata in dettaglio nella fig. 3): improbabile, moderatamente probabile, probabile, molto probabile, certo/imminente.
Infine, il "Livello di Rischio" è definito dalla *Matrice dei Rischi* (riportata in fig. 4) secondo la seguente classificazione: accettabile, medio, inaccettabile.
Per ciascun "Livello di Rischio" è stabilita la necessità di *intervento di mitigazione*, secondo quanto riportato in fig. 5.
Tale intervento può comportare opzioni:
- organizzative (con riferimento al personale impiegato nel sito);
- operative (con riferimento alle procedure adottate nel sito);
- tecnologiche (con riferimento ai dispositivi tecnologici adottati nel sito).

Nel nono capitolo vengono forniti gli elementi di valutazione per il *Crisis Management*, da adottarsi da parte dell'Operatore in caso di evento ostile verso l'Infrastruttura Critica e che deve prevedere un piano di deleghe e di livelli autorizzativi (al fine di garantire una certa operatività dell'Infrastruttura), un *Contingency Plan* (per le operazioni di emergenza) e un *Piano di Comunicazione* (verso l'interno e l'esterno dell'Infrastruttura).
Infine, il decimo capitolo definisce le modalità di esposizione dei risultati della valutazione all'Operatore responsabile dell'Infrastruttura Critica da parte del Gruppo di Valutazione, con la formulazione delle eventuali raccomandazioni di intervento. In particolare, il Responsabile del Gruppo di Valutazione concorda con l'Operatore dell'Infrastruttura un piano di intervento per l'implementazione delle azioni definite (descrizione, tempistica e responsabile per le singole attività) e per la loro verifica periodica.

[4] Si definisce "impatto" il livello di pregiudizio sull'operatività dell'Infrastruttura Critica e sul contesto sociale/ambientale/patrimoniale/economico ad essa riferibile a seguito del verificarsi di un evento ostile.
[5] Si definisce "probabilità" il livello della possibilità di accadimento di un evento ostile.

4. Conclusioni

La metodologia introdotta attraverso tale "Protocollo di Valutazione", sviluppata alla luce del citato D.Lgs.61/2011 relativo alle Infrastrutture Critiche Europee (ma di fatto applicabile a qualsiasi Infrastruttura Critica), consente pertanto di realizzare una combinazione sinergica dei tre elementi fondamentali (uomo, tecnologie, procedure) nel complesso sistema di protezione da rischi derivanti da atti di sabotaggio e terrorismo, ponendosi come efficace e dinamico strumento di Security Governance.

5. Rif. normativi e bibliografici

Direttiva 2008/114/EC – Identificazione e designazione delle Infrastrutture Critiche Europee e valutazione della necessità di elevarne il grado di protezione
D.Lgs. 61/2011 – Recepimento per l'Italia della Direttiva 2008/114/EC
Legge 155/2005 – Misure urgenti per il contrasto del terrorismo internazionale
ISO 31000:2009 – Risk Management – Principles and Guidelines
ISO 31010:2009 – Risk Management – Risk Assessment Techniques
ISO/IEC Guide 73:2002 – Risk Management – Vocabulary
United Nations – Guidelines for Security Risk Management – 24th June 2004
United Nations – Security Risk Management – Learning Module – Ed. 2009
United Nations – Minimum Operating Security Standards – 21st July 2004
United Nations – Guidelines for Security in the Field – Ed. 2008
United Nations – Field Security Handbook – Ed. 2006
US/Department for Homeland Security – Risk Assessment Methodology – Report for Congress – 2nd February 2007
US/Department for Homeland Security – Personnel Security Guidelines – Ed. 2004
UK/Centre for the Protection of National Infrastructure – Risk Assessment for Personnel Security – 3rd edition

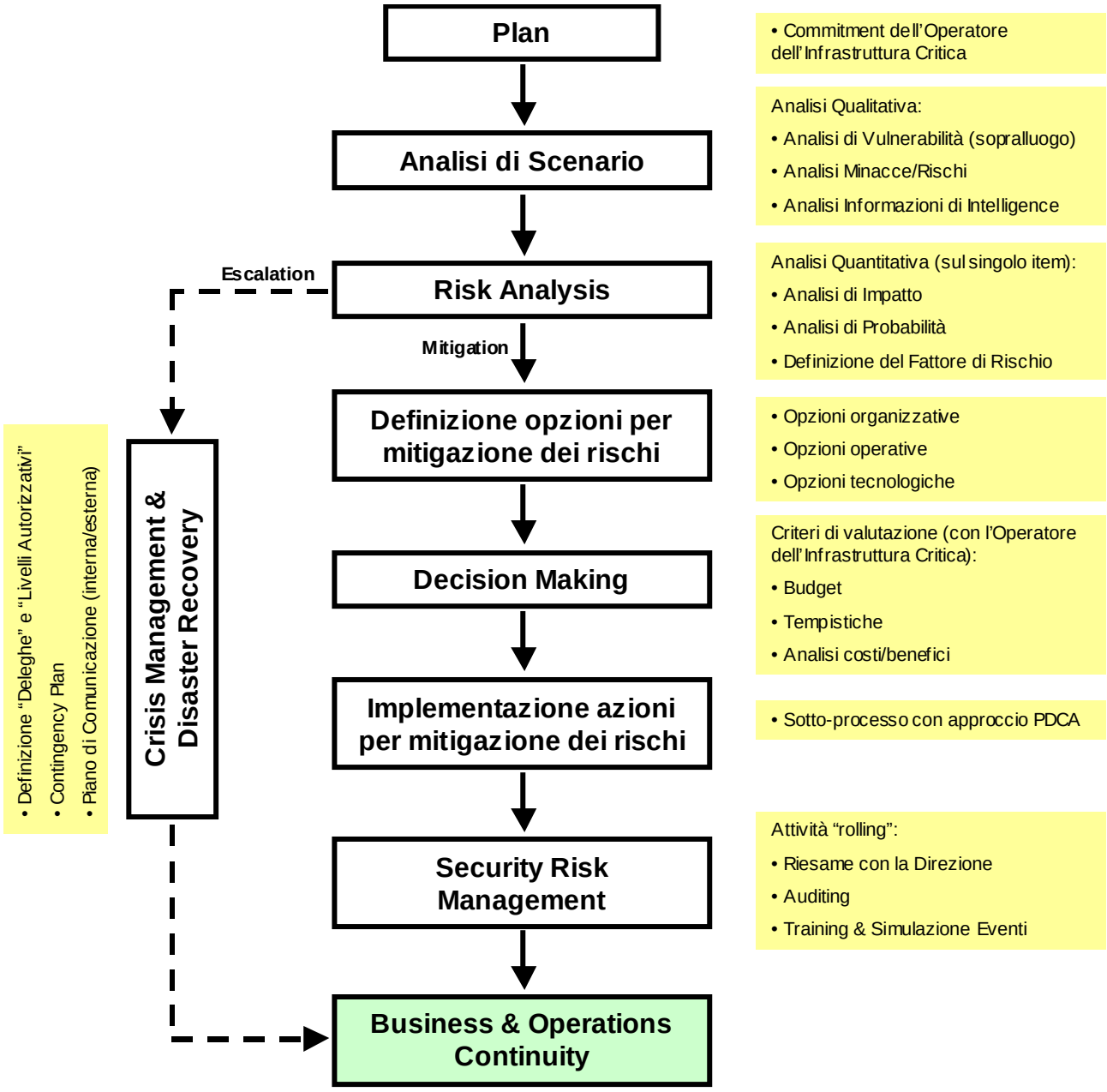

Fig. 1 – Attività di Valutazione dei Rischi Sicurezza AS/AT

Valutazione	Criterio
Trascurabile	Le conseguenze possono consistere in interruzioni di breve durata di alcune attività senza sensibili danni economici per l'Organizzazione.
Minore	Le conseguenze possono consistere in ferite di piccola entità del personale dell'Organizzazione, danneggiamento di beni strumentali e ritardi delle attività con limitati danni economici per l'Organizzazione.
Moderato	Le conseguenze possono consistere in ferite di piccola entità del personale dell'Organizzazione, danneggiamento di beni strumentali, perdite di informazioni sensibili e ritardi delle attività con sensibili danni economici per l'Organizzazione.
Severo	Le conseguenze possono consistere in ferite di grave entità del personale dell'Organizzazione, perdite di beni strumentali, perdite di informazioni sensibili e cancellazioni delle attività con gravi danni economici per l'Organizzazione.
Critico	Le conseguenze possono consistere in ferite di grave entità e decessi del personale dell'Organizzazione, perdite di beni strumentali, perdite di informazioni sensibili e cancellazione completa delle attività con gravissimi danni economici e di immagine per l'Organizzazione.

Fig. 2 – Valutazione dell'impatto dell'evento ostile

Valutazione	Criterio
Improbabile	L'evento è considerato senza una realistica probabilità di accadimento.
Moderatamente probabile	L'evento è considerato con una ragionevole probabilità di accadimento.
Probabile	L'evento è considerato con un'alta probabilità di accadimento.
Molto probabile	L'evento è considerato con una probabilità molto alta di accadimento.
Certo/Imminente	L'evento è considerato di imminente accadimento.

Fig. 3 – Valutazione della probabilità dell'evento ostile

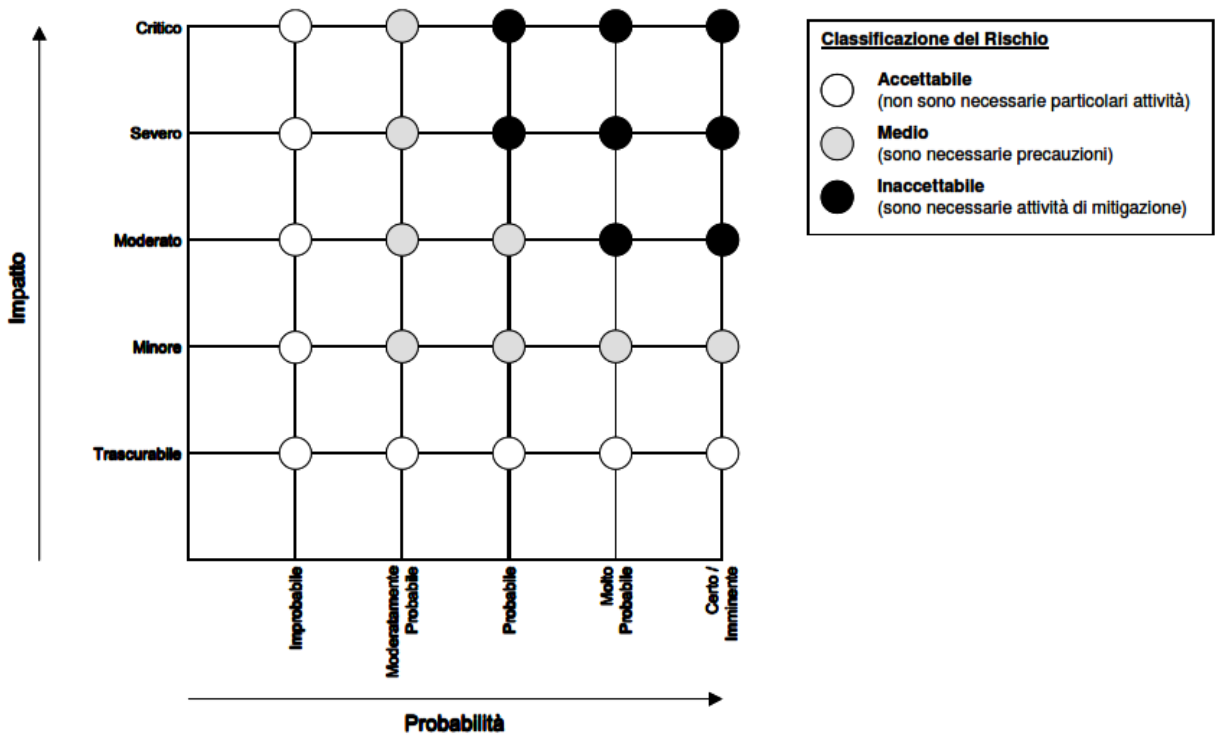

Fig. 4 – Matrice dei Rischi

Livello di Rischio	Necessità/priorità di intervento
Accettabile	Non sono necessarie particolari attività
Medio	Sono necessarie precauzioni (attività non prioritarie)
Inaccettabile	Sono necessarie attività di mitigazione (attività prioritarie)

Fig. 5 – Livello di Rischio