Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della protezione della popolazione UFPP

Guida alla protezione delle infrastrutture critiche

Impressum

Editore

Ufficio federale della protezione della popolazione
Monbijoustrasse 51a
3003 Berna

L'Ufficio federale della protezione della popolazione è grato per qualsiasi osservazione o suggerimento (ski@babs.admin.ch).

Maggiori informazioni sulla protezione delle infrastrutture critiche si trovano nel sito www.infraprotection.ch

Versioni

Versione	Data	Osservazioni
1.0	30.5.2015	
1.1	17.12.2018	Adeguamento della scala delle classi di danni; diverse modifiche redazionali (in particolare in relazione all'aggiornamento della strategia PIC).

Disclaimer

La Guida PIC si basa su norme e standard invalsi nel campo della gestione dei rischi, delle emergenze, delle crisi e della continuità operativa e le raccoglie nell'ottica di un approccio integrale alla protezione delle infrastrutture critiche. Le raccomandazioni corrispondono allo stato delle conoscenze al momento della stesura del documento. Alla luce di nuovi sviluppi potrebbero a un dato momento risultare superate, senza che il documento sia nel frattempo stato aggiornato. La guida non è giuridicamente vincolante. L'Ufficio federale della protezione della popolazione (UFPP) presta grande attenzione alla correttezza delle informazioni pubblicate. Ciononostante non può fornire garanzie sull'attualità e sulla completezza dei contenuti e declina qualsiasi responsabilità per danni materiali o immateriali derivanti dall'applicazione oppure, viceversa, dall'inosservanza delle informazioni pubblicate.

Indice

Riassunto

Per infrastrutture critiche (IC) s'intendono sistemi d'approvvigionamento, processi e installazioni essenziali per il funzionamento dell'economia e il benessere della popolazione. Vi rientrano ad esempio l'approvvigionamento energetico, i trasporti (persone e merci) e l'assistenza medica. Importanti interruzioni dell'approvvigionamento di elettricità, del traffico ferroviario o dell'approvvigionamento di beni alimentari possono avere conseguenze anche gravi. Uno degli obiettivi principali della strategia nazionale per la protezione delle infrastrutture critiche varata dal Consiglio federale nel giugno 2012 e aggiornata nel 2017, è la verifica e il miglioramento della resilienza (capacità di resistenza e rigenerazione). La presente guida descrive il relativo procedimento.

Lo scopo principale della guida è evitare, nel limite del possibile, gravi interruzioni e aiutare a ridurre al minimo i tempi d'interruzione in caso d'evento. La guida mira inoltre a instaurare una migliore cultura e comprensione dei probabili rischi.

Dal punto di vista metodologico la guida si orienta a concetti della gestione dei rischi, delle crisi e della continuità operativa invalsi e combina diversi elementi di questi approcci nell'ottica di una protezione integrale. La guida si basa su pianificazioni analoghe già in uso in molte imprese. Mentre queste ultime sono in genere focalizzate sui rischi per l'impresa, nell'ambito della protezione delle infrastrutture critiche l'accento è posto sulle conseguenze per la popolazione e le sue basi vitali (economiche) in caso di interruzioni o perturbazioni delle infrastrutture critiche.

La guida funge da ausilio per la verifica di eventuali rischi e l'identificazione delle lacune. L'intenzione non è quella di raggiungere una protezione completa e, in quanto tale, sproporzionata, da qualsiasi minaccia.

La guida intende piuttosto far sì che i costi delle eventuali misure supplementari necessarie siano proporzionali ai loro benefici. L'approccio basato sui rischi mira inoltre a evitare disparità di trattamento o distorsioni del mercato all'interno e tra i diversi settori.

L'applicazione della guida PIC richiede una stretta collaborazione tra i gestori delle infrastrutture critiche e le rispettive autorità specializzate, di vigilanza e di disciplinamento a livello federale, cantonale e comunale. Queste sono responsabili di creare le condizioni quadro per il buon funzionamento delle infrastrutture critiche nei vari settori. Nei diversi ambiti politici (politica energetica, politica dei trasporti, sanità pubblica, ecc.) dovrà invece essere chiarita l'attuazione e il finanziamento delle misure supplementari eventualmente necessarie.

I gestori possono utilizzare la guida anche senza coinvolgere le autorità. Essi possono così verificare se sussistono eventuali rischi di interruzioni con gravi ripercussioni sulla società e sull'economia che potrebbero minacciare anche la sopravvivenza stessa dell'impresa.

1 Introduzione

1.1 Situazione iniziale

Infrastrutture critiche

Le infrastrutture critiche (IC)[1] garantiscono la disponibilità di beni e servizi importanti quali l'energia, le telecomunicazioni e i trasporti. Perturbazioni, interruzioni e distruzioni di infrastrutture critiche possono avere gravi conseguenze per la popolazione e le sue basi vitali.

Le infrastrutture critiche sono suddivise in settori e sottosettori (per es. corrente elettrica, gas e petrolio nel settore energetico)[2]. Fondamentalmente, all'interno dei singoli sottosettori critici occorre considerare come parte dell'infrastruttura critica tutti gli elementi dell'oggetto (per es. azienda operatrice, impianti, sistemi, ecc.), distinguendone la relativa importanza (o la criticità)[3].

Strategia nazionale PIC

L'8 dicembre 2017, il Consiglio federale ha varato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC) 2018 – 2022 [4]. Questa sostituisce la Strategia nazionale PIC del 2012.

La Strategia nazionale PIC 2018 – 2022 stabilisce i principi, le definizioni e gli obiettivi principali per una protezione completa della Svizzera nell'ambito delle infrastrutture critiche. Essa serve agli organi coinvolti a livello federale e comunale come pure ai gestori delle infrastrutture critiche come quadro di riferimento per lo svolgimento dei lavori specifici in campo PIC.

La strategia definisce complessivamente 17 misure, come ad esempio l'allestimento di un inventario delle infrastrutture critiche periodicamente aggiornato (Inventario PIC). Altre misure prevedono ad esempio l'elaborazione di pianificazioni d'intervento preventive da parte dei partner nella protezione della popolazione e dell'esercito. Uno dei punti cardine della strategia è la verifica e il miglioramento della resilienza delle infrastrutture critiche di per sé. A tal fine il Consiglio federale, con la misura M 1 ha incaricato i gestori di infrastrutture critiche di verificare la loro resilienza (capacità di resistenza e di rigenerazione) e di migliorarla se necessario.

La presente guida costituisce un ausilio prezioso per l'attuazione delle misure; spiega di quali punti occorre tenere conto e come procedere. A complemento di tali lavori il Consiglio federale ha incaricato le varie autorità specializzate, di sorveglianza e di regolazione nei diversi settori di verificare in tutti i sottosettori se sussistono dei rischi per una grave interruzione e se necessario di adottare le misure per ridurli. A tal fine si applica un procedimento analogo a quello previsto dalla guida PIC.

Lavori preliminari

In diversi sottosettori sono già disponibili direttive e pianificazioni per la protezione delle infrastrutture critiche. Tuttavia, nella maggior parte dei casi queste si riferiscono solo a singoli aspetti (per es. la protezione da pericoli derivanti dall'infrastruttura, sicurezza della produzione, garanzia d'approvvigionamento sul lungo termine, protezione da singole minacce, ecc.). D'altronde, ai sensi di una *protezione integrale*, questa guida tiene conto sia di un ventaglio molto ampio di minacce, sia di un ventaglio molto ampio di misure. Ciò significa che occorre tener

[1] Per una definizione dettagliata cfr. → Spiegazione dei termini
[2] Cfr. allegato 7 – Panoramica dei settori e sottosettori critici
[3] Per questo motivo non è possibile operare una distinzione tra "critico" e "non critico" all'interno dei singoli sottosettori. Nel sottosettore «corrente elettrica» occorre ad esempio considerare gestori di infrastrutture critiche tutte le 900 imprese di approvvigionamento di corrente elettrica, ovviamente distinguendone l'importanza: alcune sono rilevanti a livello nazionale, mentre (molte) altre solo a livello comunale o locale.
[4] La «Strategia nazionale per la protezione delle infrastrutture critiche 2018-2022» (FF 2018 455-492) è disponibile nella pagina PIC di www.infraprotection.ch.

conto di tutte le minacce *rilevanti* che potrebbero causare interruzioni o perturbazioni. Il ventaglio delle misure comprende tutte le misure idonee di natura edilizia, tecnica e organizzativa, volte a evitare le interruzioni e ridurne i tempi in caso d'evento. Anche i gestori delle infrastrutture critiche (gestori IC) dispongono, di regola, di pianificazioni complete in relazione alla protezione e alla sicurezza dell'impresa. In base al diritto delle obbligazioni, aziendale e societario, molte imprese sono ad esempio tenute ad applicare una gestione dei rischi e dunque un sistema di controllo interno efficace. Molte imprese dispongono inoltre di pianificazioni volte a garantire la continuità operativa (Business Continuity Management, BCM). La presente guida è concepita in modo tale da orientarsi a questi processi dal punto di vista metodologico e garantire che si possa tenere conto dei relativi lavori (cfr. capitolo 2), riducendo così notevolmente gli oneri per le imprese. Nell'ambito dei lavori preliminari, direttive, accordi, misure, ecc. esistenti vengono rilevati in modo mirato (vedi capitolo 3.1.3) e presi in considerazione durante l'analisi dei rischi. Se sono già state implementate numerose misure di sicurezza, ciò si manifesterà sotto forma di un minore margine di rischio, riducendo inoltre la necessità di adottare delle misure supplementari.

1.2 Guida PIC

Genesi

La guida è stata elaborata in stretta collaborazione con il gruppo di lavoro interdipartimentale PIC (GL PIC)[5], in cui sono rappresentati 26 enti federali e due cantoni. L'elaborazione della guida è stata seguita da un gruppo composto da esperti nei settori della gestione dei rischi, delle emergenze, delle crisi e della continuità operativa.

Nel settembre del 2011 si è inoltre tenuto un workshop con la collaborazione del Politecnico federale dei Zurigo in occasione del quale la guida è stata testata e valutata da esperti nei settori sopraccitati e da rappresentanti dell'economia privata, del mondo scientifico e da diverse associazioni di categoria.

Nel 2012 e 2013 è stata testata l'utilità pratica della guida in collaborazione con un gestore IC dapprima su un oggetto IC concreto, e in un secondo tempo applicandola ai principali processi aziendali sull'arco di diversi mesi.

Nella primavera del 2014 la guida è stata infine sottoposta per consultazione ad associazioni specializzate, ai gestori IC, alle conferenze cantonali e ancora una volta al GL PIC.

Scopo

La presente *Guida alla protezione delle infrastrutture critiche* è uno strumento atto a verificare ed eventualmente migliorare la resilienza delle infrastrutture critiche. Essa è concepita in particolare per l'applicazione nei sottosettori critici e a livello d'esercizio degli oggetti iscritti nell'Inventario PIC[6].

---

[5] Enti federali: Cancelleria federale (CaF), Divisione politica di sicurezza (DPS-DFAE), Direzione dello sviluppo e della cooperazione (DSC), Ufficio federale della sanità pubblica (UFSP), Ufficio federale di meteorologia e climatologia (MeteoSvizzera), Ufficio federale di polizia (fedpol), Politica di sicurezza DDPS (POLSIC DDPS), Servizio delle attività informative della Confederazione (SIC), Protezione delle informazioni e delle opere (PIO), Comando, operazioni, armasuisse immobili (ar Immo), ufficio federale della protezione della popolazione (UFPP), Amministrazione federale delle finanze (AFF), Ufficio federale delle costruzioni e della logistica (UFCL), Ufficio federale dell'informatica e della telecomunicazione (UFIT), Organo direzione informatica della Confederazione (OIDIC, Ufficio di coordinamento strategia nazionale rischi informatici), Ufficio federale per l'approvvigionamento economico del Paese (UFAE),, Ufficio federale dei trasporti (UFT), Ufficio federale dell'aviazione civile (UFAC), Ufficio federale dell'energia (UFE), Ufficio federale delle strade (USTRA), Ufficio federale delle comunicazioni (UFCOM), Ufficio federale dell'ambiente (UFAM), Commissione federale dell'energia elettrica (ElCom), Ispettorato federale della sicurezza nucleare (IFSN). Cantoni: Canton Ginevra, Canton Basilea-Città.

[6] L'Inventario PIC riporta un elenco degli oggetti d'importanza strategica per la Svizzera e offre tra l'altro una panoramica comparativa sull'importanza dei vari oggetti. Funge da base per la pianificazione e

La guida PIC mira a ridurre la probabilità d'insorgenza di perturbazioni o interruzioni di ampia portata e lunga durata alle infrastrutture critiche, nonché a limitare l'entità dei danni e il tempo d'interruzione in caso d'evento. L'obiettivo è di proteggere le infrastrutture critiche in modo ottimale, cioè di applicare misure adeguate al rischio rappresentato dalle stesse IC. Non si aspira invece a una protezione completa da qualsiasi rischio, poiché ciò sarebbe in contrasto con i principi di procedura e proporzionalità basate sul rischio prescritte dalla strategia PIC nazionale.

La guida PIC si prefigge inoltre di instaurare una migliore cultura e comprensione dei potenziali rischi. Gli insegnamenti tratti dai procedimenti illustrati devono anche essere utilizzati per completare le misure di protezione mancanti o insufficienti. Se ne deve inoltre tenere conto nelle strutture interne esistenti di gestione dei rischi, delle emergenze, delle crisi e della continuità operativa aziendali.

Destinatari

La protezione delle infrastrutture critiche è un compito collettivo che richiede una stretta collaborazione tra gestori IC e autorità specializzate, di vigilanza e di regolazione competenti. La guida si rivolge quindi sia ai gestori delle infrastrutture critiche, sia alle autorità competenti. La guida può essere applicata:

1. dai gestori delle infrastrutture critiche, che sono responsabili di garantire un funzionamento possibilmente privo di perturbazioni dei loro impianti e che intendono applicare la guida sotto la propria responsabilità.
2. dai servizi specializzati a livello federale, cantonale o comunale che in base alla legislazione vigente svolgono un ruolo di gestione o vigilanza delle rispettive infrastrutture critiche. La guida può aiutarle a chiarire se sussistono dei rischi per la società e l'economia che richiedono misure a livello legislativo, di regolazione o simile da parte delle autorità.

Dato che le singole misure di protezione delle infrastrutture critiche possono risultare piuttosto onerose dal punto di vista finanziario, per l'applicazione della guida e in particolare per la valutazione di possibili misure si raccomanda di cercare la collaborazione con altri gestori. Spesso è infatti possibile ridurre i rischi in modo economico ed efficace rafforzando la cooperazione (per es. sotto forma di un'organizzazione comune di crisi), acquisendo e utilizzando le risorse in modo congiunto. Le diverse associazioni di categoria possono svolgere un ruolo importante nel coordinamento dei lavori.

Valore aggiunto per i gestori IC

Grazie all'applicazione della guida i gestori delle IC ottengono un valore aggiunto a diversi livelli per quanto riguarda la protezione delle IC:

- la guida fornisce le basi decisionali per un impiego efficiente dei mezzi (minimo investimento per massimo accrescimento della sicurezza);
- aiuta i gestori a spiegare le prestazioni fornite a favore della popolazione e dell'economia, e a valutare, assieme alle autorità competenti, le misure necessarie per assicurare queste prestazioni;
- promuove l'«unità di dottrina» e la compatibilità delle misure all'interno e tra i diversi settori delle infrastrutture critiche in riferimento alla protezione integrale;
- permette, grazie a un'applicazione generalizzata, un'elevata disponibilità delle infrastrutture critiche in Svizzera, da cui traggono profitto soprattutto le aziende stesse (vantaggio d'ubicazione).

---

la presa di decisione nell'ambito della gestione dei rischi, delle crisi e delle catastrofi a livello di Confederazione, Cantoni e gestori delle infrastrutture. Nel suo insieme è classificato come SEGRETO, singoli estratti di regola come CONFIDENZIALI.

Contesto

La guida non sostituisce né prevarica alcuna disposizione vigente in relazione alla protezione delle infrastrutture critiche. Si tratta piuttosto di un complemento a lavori in corso o già esistenti in questo settore. Dal punto di vista metodologico la guida si rifà a sistemi di gestione invalsi (cfr. capitolo 2). L'elaborazione e la realizzazione di sistemi e strumenti supplementari è fortemente sconsigliata.

2 Presupposti

2.1 Interfacce con sistemi di gestione invalsi

La guida presenta delle interfacce con diversi sistemi di gestione invalsi a livello aziendale. Per esempio:

- gestione della sicurezza
- gestione dei rischi
- gestione della continuità operativa (ingl. «*Business Continuity Management*», BCM)
- gestione delle crisi
- gestione delle emergenze
- sistema di controllo interno (SCI)

Negli standard, nelle norme e nella letteratura i sistemi di gestione citati sono spesso definiti in modo diverso. A seconda dell'organizzazione, i vari sistemi sono trattati singolarmente, oppure integrati come sottosistemi in altri sistemi. L'importante è che ciascuna delle componenti consideri diversi aspetti e che si completino a vicenda per migliorare la sicurezza nell'azienda, al fine di ottenere una diminuzione della probabilità, rispettivamente dell'entità delle perturbazioni. Per garantire una protezione ottimale è indispensabile tenere conto di tutti gli aspetti della sicurezza aziendale. Spetta alla relativa organizzazione decidere come conciliare i singoli sistemi tra loro.

La presente guida non si prefigge né pretende di fornire una definizione universalmente valida dei sistemi, né di delimitarli l'uno dall'altro secondo criteri ben determinati. Per comprendere pienamente la guida e l'interazione tra le diverse componenti, i suddetti sistemi di gestione sono brevemente esposti nel paragrafo «Spiegazione dei termini» tenendo conto delle definizioni scelte.

Sistemi di gestione particolarmente importanti per la PIC

Tra i sistemi di gestione succitati, sono due quelli che rivestono particolare importanza per la PIC: la gestione dei rischi (aspetto «evitare gli eventi») e la gestione della continuità operativa (aspetto «preparazione in vista di eventi»). Dal momento che le opinioni su come definire e distinguere tra loro i due sistemi risultano divergenti, nel presente documento si rinuncia a fornire una definizione univoca dei due approcci. Riportiamo invece le principali norme e direttive in materia, a titolo informativo per gli organi interessati.

Settore tematico	Basi
Gestione dei rischi	*Istruzioni e indicazioni per l'attuazione di una gestione dei rischi si trovano per es. nei documenti seguenti:* *- ISO 31000 Gestione integrata dei rischi* *- ONR 49001 ss. Applicazione delle norme ISO 31000 nella pratica* *- HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004* *- Handbuch zum Risikomanagement Bund (Manuale per la gestione dei rischi della Confederazione)*
Misure volte a garantire la continuità operativa	*Istruzioni e indicazioni per l'attuazione di una gestione della continuità operativa si trovano per es. nei documenti seguenti:* *- ISO 22301: Societal Security – Business Continuity Management Systems – Requirements* *- ISO 22313: Societal Security – Business Continuity Management Systems – Guidance. First edition, 15 dicembre 2012* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- Guida BCM dell'Ufficio federale dell'approvvigionamento economico del Paese («Nessuna brutta sorpresa per la mia impresa»)* *- HB 221/2004 Business Continuity Management (in base a AS/NZS)*

Tabella 1: Documenti di base per settore tematico

2.2 Approccio della guida

Ampliare l'orizzonte

Applicare la presente guida non significa introdurre un ulteriore sistema di gestione all'interno dell'azienda. Si tratta piuttosto di partire dai sistemi esistenti per ampliarli nell'ottica della protezione delle infrastrutture critiche. Mentre i sistemi convenzionali sono focalizzati sui rischi per l'impresa o per l'organizzazione, in ambito PIC ci si concentra sui rischi per la popolazione e le sue basi vitali.

Per **basi vitali** s'intende l'insieme degli elementi di cui la popolazione ha bisogno per vivere. *Le basi vitali rendono possibile la convivenza collettiva e individuale. Si possono suddividere in basi vitali naturali, economiche e sociali.*

- *Basi vitali naturali:*
  ambiente intatto (suolo, acque, aria, biodiversità)
- *Basi vitali economiche:*
  economia florida e infrastrutture funzionanti
- *Basi vitali sociali:*
  sistema giuridico, sanitario e educativo (formazione, ricerca) funzionante, fiducia della popolazione nelle istituzioni statali, integrità territoriale e diversità culturale

I sistemi di gestione dei rischi (aziendali) e della continuità operativa invalsi mettono in primo piano i rischi e i processi che sono importanti per il successo (di regola economico) dell'impresa. La guida PIC è invece incentrata sui rischi e sui processi importanti per la comunità. È possibile che vi siano delle intersezioni tra i due punti di vista, ma difficilmente saranno identici.

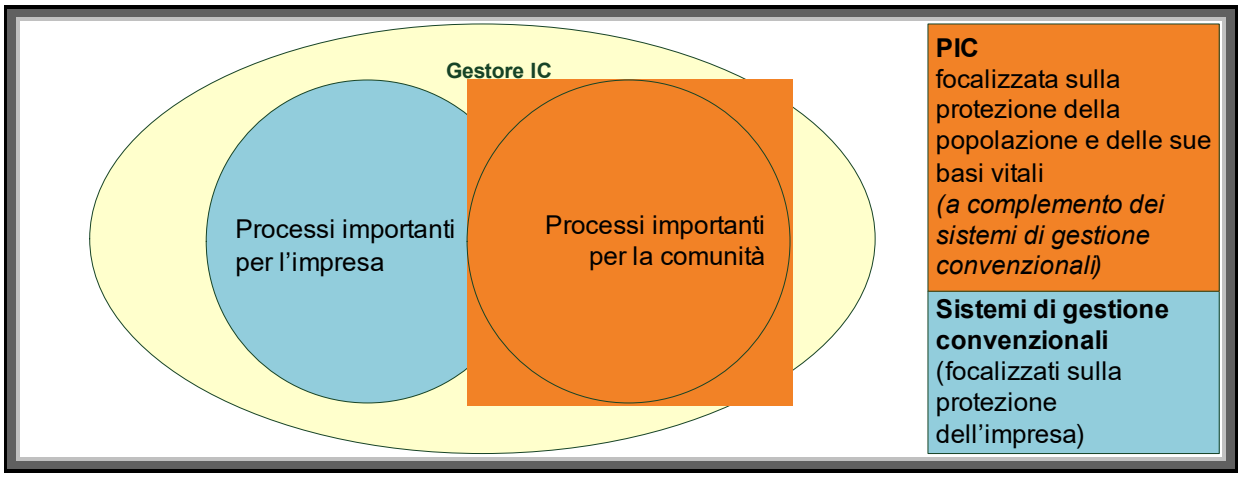


Figura 1: *La protezione delle infrastrutture critiche (PIC) come complemento ai sistemi di gestione convenzionali già implementati nelle imprese – Gli strumenti rimangono gli stessi, ma viene ampliato il target di riferimento.*

Esempio: per molte imprese rivestono grande importanza i processi e i rischi nel campo della riscossione. In caso di cattivo o mancato funzionamento di questa attività, la popolazione e l'economia non sono però direttamente interessati. Al contrario, un processo dell'approvvigionamento (economico) di base può risultare insignificante dal punto di vista dell'impresa, ma essere di fondamentale importanza per l'economia e la popolazione.

Anche se dal punto di vista metodologico la guida PIC si basa su questi strumenti, soprattutto sulla gestione dei rischi e della continuità operativa, non può essere equiparata a questi ultimi.

2.3 Ruoli e collaborazione

L'applicazione della guida PIC richiede una stretta collaborazione trai i gestori e le autorità specializzate competenti a livello federale, cantonale ed eventualmente comunale. Ma anche le associazioni di categoria possono assumere un'importanza significativa. I seguenti ruoli e le seguenti funzioni sono di principio possibili:

Ruolo	Funzione
Gestori IC	➢ Dirigere l'applicazione della guida ➢ Integrare le conoscenze dell'impresa ➢ Applicare le misure nell'ambito dell'esercizio delle IC
Associazioni di categoria	➢ Coordinare e rappresentare gli interessi dei gestori ➢ Eventuale collaborazione durante l'elaborazione di soluzioni settoriali
Autorità	➢ Raccomandare i gestori IC ad applicare la guida PIC ➢ Accompagnare / sostenere il processo a livello politico ➢ Disciplinare l'attuazione e il finanziamento delle eventuali misure supplementari necessarie

Tabella 2: Ruoli e funzioni

La collaborazione con le autorità e lo scambio reciproco all'interno e tra settori analoghi sono opportuni per i seguenti motivi:

- Di regola nei vari sottosettori critici sono diversi i gestori interessati dalla guida PIC. Le associazioni di categoria agevolano il coordinamento e rappresentano gli interessi dei singoli gestori di fronte alle autorità di vigilanza e di regolazione. Potrebbe inoltre offrirsi la possibilità di regolare eventuali misure supplementari necessarie nei sottosettori (per es. sotto forma di una migliore collaborazione e di sostegno reciproco in caso d'evento). Ciò permetterebbe di ridurre notevolmente gli oneri delle singole imprese (sia nell'applicazione della guida, sia in relazione ad eventuali misure supplementari necessarie).
- Determinate misure di protezione ritenute appropriate per le infrastrutture critiche potrebbero risultare insostenibili dal punto di vista economico per i gestori. Coinvolgendo le associazioni di categoria e le autorità specializzate competenti si garantisce che il finanziamento nell'ambito del rispettivo settore politico (per es. politica energetica, politica dei trasporti, ecc.) sia assicurato.

3 Protezione integrale delle infrastrutture critiche

Il procedimento per la protezione integrale delle infrastrutture critiche si basa su un processo sistematico continuo (vedi figura 2):

Figura 2: Processo per la protezione integrale delle infrastrutture critiche

Dopo una fase di preparazione, in cui vengono chiarite le responsabilità ed assegnate le competenze e gli incarichi, segue un processo iterativo in cinque fasi volto a migliorare la protezione delle infrastrutture critiche.

Nella prima fase di analisi si identificano i processi critici e si analizzano le minacce che possono portare a una perturbazione di questi processi. In seguito, i rischi risultanti vengono rilevati e confrontati tra loro.

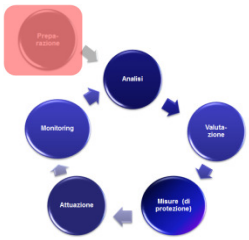
Nella seconda fase si procede alla valutazione dei rischi e delle vulnerabilità.

Nella terza fase vengono valutate le misure che permettono di ridurre efficacemente i rischi.

La quarta fase prevede l'attuazione delle misure. La guida spiega come vengono pianificate, attuate, accompagnate e sorvegliate.

Nella quinta fase si procede alla verifica e al controllo (monitoring), ossia alla verifica e al miglioramento delle misure. In questo modo è possibile osservare costantemente i progressi dell'attuazione delle misure e la loro reale efficacia.

3.1 Preparazione



Una preparazione accurata è il presupposto per un'applicazione riuscita della guida PIC. Prima di procedere occorre infatti chiarire alcuni aspetti fondamentali. Vi rientrano in particolare l'assegnazione degli incarichi, l'istituzione e l'organizzazione di un gruppo di lavoro, la determinazione delle competenze e la messa a disposizione delle risorse necessarie allo svolgimento dei lavori.

3.1.1 Sostegno da parte del livello direttivo e assegnazione degli incarichi

Considerate l'importanza e la portata delle conseguenze delle decisioni richieste, è necessario che l'applicazione della guida sia sostenuta dall'organo direttivo dell'impresa (direzione, consiglio d'amministrazione, ecc.). Questo è responsabile del funzionamento mirato ed efficiente di tutti i settori aziendali, del fatto che i rischi vengano riconosciuti e ridotti e che le conseguenze per l'impresa in caso d'incidente siano ridotti al minimo[7].

Anche se singoli compiti legati all'applicazione della guida vengono delegati, assieme alle relative responsabilità, a collaboratori o unità organizzative, non si può delegare la responsabilità generale che deve rimanere del rispettivo organo direttivo. L'organo direttivo deve assicurare che vengano messe a disposizione risorse sufficienti (personale, tempo, mezzi finanziari) per l'attuazione della guida.
L'organo direttivo responsabile deve formulare un incarico chiaro per l'applicazione della guida. Questo deve contenere i punti seguenti:

- importanza del progetto per il gestore IC
- obiettivi del progetto
- campo d'applicazione del progetto
- struttura del gruppo di lavoro incaricato del progetto, con ruoli principali e rispettive competenze
- risorse disponibili (tempo, personale, mezzi finanziari, ecc.)

3.1.2 Rilevamento di lavori preesistenti

Nell'ampio contesto della protezione delle infrastrutture critiche, esistono di regola già numerosi lavori che trattano singoli aspetti PIC. L'applicazione della guida PIC si basa in larga misura sui lavori e sulle pianificazioni già esistenti. Esempi di lavori già esistenti sono:

Internamente:

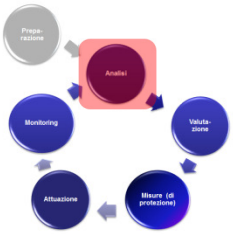
- lavori nel campo della gestione dei rischi, delle emergenze, delle crisi e della continuità operativa
- sistemi di gestione implementati, compresi i processi
- strumenti di condotta implementati
- prescrizioni, direttive e standard interni

Esternamente:

- basi e disposizioni legali in materia
- standard e soluzioni valide per tutto il settore
- norme, direttive e guide d'applicazione
- strategia nazionale PIC, Inventario PIC e strutture funzionali elaborate in questo contesto (contiene tra l'altro indicazioni relative a processi e agli elementi critici)
- rapporti e studi specifici per il sottosettore in relazione alla prevenzione degli incidenti e alla riduzione dei danni in caso d'evento

[7] Vedi a riguardo anche l'articolo 55 del codice delle obbligazioni svizzero.

3.2 Analisi



Nella fase di analisi vengono definiti i processi critici, accertate le minacce rilevanti e i punti vulnerabili ed identificati i relativi rischi.

Il seguente schema illustra le singole tappe di questo capitolo:

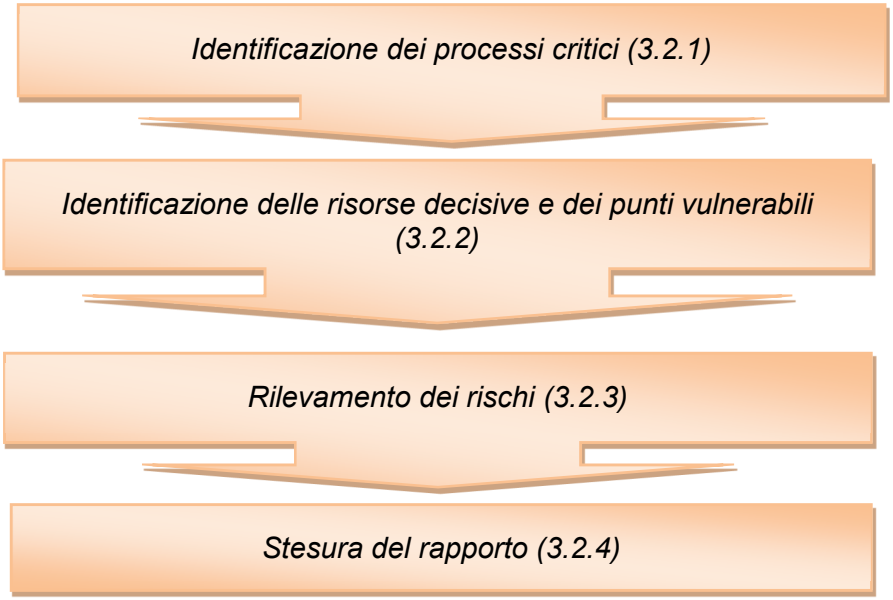


Figura 3: Schema delle varie tappe della fase di analisi

3.2.1 Identificazione dei processi critici

Il presupposto principale per garantire una protezione possibilmente completa di un'infrastruttura critica è una conoscenza approfondita del suo scopo e delle sue funzioni. Per questo occorre comprendere quali sono i processi indispensabili per garantire un funzionamento minimo dell'infrastruttura critica.

L'identificazione dei processi critici si basa in larga misura sull'analisi completa dei principali processi aziendali nell'ambito della gestione della continuità operativa (*Business Impact Analysis*). Se ciò non fosse ancora stato fatto, le relative norme e direttive (cfr. tabella 1) forniscono le informazioni necessarie sul modo di procedere.

*Nell'ambito della protezione delle infrastrutture critiche, per **processo critico** s'intende un processo essenziale per il funzionamento dell'infrastruttura critica, la cui interruzione avrebbe ripercussioni gravi ed immediate sulla popolazione e le sue basi vitali.*

Il numero di processi critici identificati dovrebbe essere il più ristretto possibile. La seguente tabella mostra un esempio **fittizio** di possibili processi critici:

N°	Processo critico
1	Produzione
2	Conduzione e gestione del sistema
3	Distribuzione

Tabella 3: Esempi di processi critici

3.2.2 Identificazione delle principali risorse e dei punti vulnerabili

Si tratta ora di valutare quali risorse sono indispensabili per svolgere i processi precedentemente identificati come critici. Occorre tenere conto in particolare delle risorse nei settori seguenti: materie prime, energia, TIC, forza lavoro, logistica e infrastruttura.

La seguente Figura 4 illustra il procedimento:

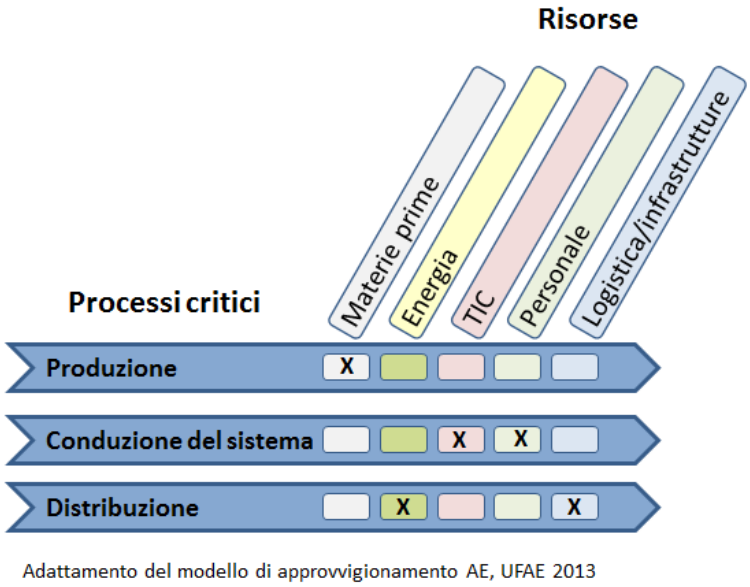


Figura 4: Modello di rapporto tra processi critici e risorse necessarie

Infine si tratta di descrivere quali conseguenze avrebbe la mancanza della relativa risorsa sul processo critico, nello specifico quanto influirebbe sullo svolgimento del processo la mancanza di questa risorsa.

3.2.3 Rilevamento dei rischi

A questo punto occorre rilevare quali rischi per la popolazione e le sue basi vitali costituiscono dei punti vulnerabili secondo la definizione data al capitolo 3.2.2.

*Il **rischio** è un metro di misura per le dimensioni di una minaccia. Può essere rappresentato come prodotto della probabilità d'insorgenza risp. della plausibilità di un evento e dell'entità dei danni che ne risulta per la popolazione e le sue basi vitali.*

Nell'ambito della protezione delle infrastrutture critiche, il concetto di «rischio» serve sia come modello per valutare gli aspetti legati alla sicurezza, sia per confrontare le diverse minacce sulla base di stessi criteri.

I due fattori centrali del rischio correlato a un sinistro sono pertanto la probabilità d'insorgenza e l'entità dei danni.

*Per **probabilità d'insorgenza** s'intende la probabilità stimata o basata su valori statistici che un evento si verifichi in un determinato lasso di tempo.*

*Con il concetto «**entità dei danni**» si definiscono le conseguenze stimate per la popolazione e le sue basi vitali in seguito al mancato funzionamento di uno o più processi critici nel caso in cui la minaccia dovesse concretizzarsi. L'entità dei danni si compone della somma dei danni al momento del verificarsi dell'evento e dei danni che possono insorgere durante l'intera fase di ripristino.*

Il rilevamento dei rischi avviene in tre passi: in un primo tempo vengono identificate le minacce rilevanti; in seguito vengono elaborati i relativi scenari, che vengono poi valutati in relazione alla loro probabilità d'insorgenza o plausibilità e all'entità dei danni per la popolazione e le sue basi vitali.

Primo passo: Scelta delle minacce rilevanti

I processi e le risorse identificati come rilevanti secondo i capitoli 3.2.1 e 3.2.2 devono essere elencati in una tabella e numerati. Per quelle risorse che si trovano nella propria sfera di competenza, occorre identificare le minacce rilevanti che potrebbero portare alla mancata disponibilità della risorsa in questione[8]. A questo scopo si deve tenere conto di un ventaglio possibilmente ampio di minacce, ossia di tutte le potenziali minacce che potrebbero portare a una significativa mancanza di questa risorsa. Come ausilio per l'identificazione è disponibile tra l'altro il catalogo dei pericoli dell'UFPP[9].

- Catalogo dei pericoli: è un elenco completo e aggiornabile dei pericoli che potrebbero minacciare la popolazione e le sue basi vitali. Il catalogo fornisce una panoramica dei potenziali eventi e sviluppi, senza tuttavia precisare l'ordine delle priorità. Il catalogo è specifico alla risorsa e deve essere completato con altri pericoli che potrebbero portare a delle interruzioni.

Per le risorse esterne (fornitori, servizi, ecc. esterni all'impresa), si tratta sempre di analizzare la mancata disponibilità della relativa risorsa, indipendentemente dalla causa. La tabella 4 mostra un esempio fittizio di catalogo dei pericoli:

[8] Risorse per le quali è possibile evitare una penuria grazie a misure preventive. Sussiste pertanto una differenza rispetto alle misure di preparazione che mirano a evitare che la mancata disponibilità di una risorsa porti a un'interruzione del processo.
[9] www.risk-ch.ch -> Catalogo dei pericoli

N°	Processi critici secondo il cap. 3.2.1	Risorse rilevanti secondo il cap. 3.2.2	Mancata disponibilità di risorse esterne / minaccia rilevante per le risorse nella propria sfera di competenza
1	Produzione	*Materie prime (esterno)*	*Penuria di materie prime*
2	Produzione	Costruzioni / impianti (stabilimento X)	Terremoto
3	Produzione	Costruzioni / impianti (stabilimento X)	Attentato convenzionale
3	Conduzione e gestione dei sistemi	*TIC (esterno)*	*Interruzione dei sistemi di telecomunicazione pubblici*
4	Conduzione e gestione dei sistemi	TIC (rete aziendale)	Attentato informatico
5	Conduzione e gestione dei sistemi	Personale (addetti alla gestione dei sistemi)	Pandemia
7	Distribuzione	*Energia (esterno)*	*Interruzione dell'approvvigionamento di elettricità*
8	Distribuzione	Costruzioni / impianti (centrale di distribuzione Z)	Incendio

Tabella 4: Esempio di confronto tra processi, risorse e minacce

Secondo passo: elaborazione degli scenari

In questo passo vengono elaborati degli scenari in cui si descrivono, mediante esempi, in che forma e in che misura viene a mancare la risorsa rilevante, quali ripercussioni ha la minaccia rilevante sulla risorsa e quali sono le conseguenze per la popolazione e le sue basi vitali. Esempi di scenari e informazioni concernenti le diverse minacce si trovano ad esempio nei lavori relativi all'analisi nazionale dei pericoli «Catastrofi e situazioni d'emergenza in Svizzera»[10].

Presupponendo che i gestori delle infrastrutture critiche siano in grado di far fronte agli eventi quotidiani e alle loro conseguenze e che questi non rappresentino quindi un problema per la comunità, gli eventi da prendere in considerazione sono quelli di intensità da elevata a estrema. I lavori si devono fondare sul principio del *credible worst case*, il peggiore dei casi ancora plausibile. Ciò significa che la minaccia presa in considerazione deve ripercuotersi nelle condizioni meno favorevoli sulla rispettiva risorsa[11]. Il tempo massimo di mancato funzionamento degli impianti (tempo necessario per la riparazione o la messa a disposizione di fonti d'approvvigionamento alternative) deve essere stimato in modo realistico, ossia tenendo conto delle condizioni quadro dei pericoli presi in esame (per es. quando a causa di un evento di ampia portata è pregiudicata anche la disponibilità di pezzi di ricambio o del personale specializzato).

[10] www.risk-ch.ch

[11] Esempio: considerata la minaccia «terremoto» e la risorsa «costruzioni e impianti» con due ubicazioni ridondanti (per es. centri di calcolo), si ipotizzerà un terremoto di forte intensità che danneggerà in ugual modo entrambe le ubicazioni.

Terzo passo: valutazione degli scenari

Si tratta ora di rilevare gli effetti dannosi che possono risultare in base ai relativi scenari. Contrariamente ai consueti approcci nell'ambito della gestione dei rischi e della continuità operativa, in questo caso non ci si focalizza sulle conseguenze per l'impresa, bensì sulle conseguenze per la popolazione e le sue basi vitali.

Per rilevare l'entità dei danni, occorre scegliere degli indicatori adeguati. Nella seguente tabella vengono proposti alcuni indicatori per stabilire i danni alla popolazione e alle sue basi vitali causati da interruzioni o da perturbazioni alle infrastrutture critiche. A seconda dell'infrastruttura esaminata è possibile che alcuni indicatori non vengano presi in considerazione o che sia necessario stabilirne altri. La scelta degli indicatori deve essere documentata e motivata nell'ambito di un rapporto.

Settore colpito	Sottosettore	Indicatore	Base costituzionale	Unità di misura
Persone	Vita e salute	**Decessi**	Art. 10, 57, 58, 61,118	Quantità
		Feriti/malati		Quantità
	Aiuto in situazioni d'emergenza	**Persone bisognose d'aiuto**	Art 12, 115	Giorni x persone impiegate
Ambiente	Ecosistema	**Ecosistemi danneggiati**	Art. 74, 76, 77, 78, 104	Superficie x anni
Economia	Patrimoni	**Danni patrimoniali e costi di gestione (beni e patrimoni finanziari)**	Art. 61	CHF
	Efficienza economica	**Diminuzione dell'efficienza economica**	Art. 100	CHF
Società	Approvvigionamento con beni e servizi vitali	**Limitazione della qualità di vita**	Art. 102	Persone x giorni
	Ordine costituzionale, sicurezza interna	**Riduzione dell'ordine pubblico e della sicurezza interna**	Art. 52, 185	Persone x giorni
	Immagine e fiducia nello Stato	**Danni all'immagine**	Art. 54	Intensità x durata
		Perdita di fiducia nello Stato e nelle istituzioni	Preambolo, art. 2, 5	Intensità x durata
	Integrità territoriale	**Violazione dell'integrità territoriale**	Art. 58	Intensità x durata
	Beni culturali	**Danneggiamento o perdita di beni culturali**	Art. 2, 69, (78)	Quantità x importanza

Tabella 5: Esempio di indicatori dei danni

Informazioni dettagliate sui singoli indicatori dei danni e proposte per le relative classi figurano nell'appendice 2 – Indicatori dei danni.

IMPORTANTE!

Per rilevare l'entità dei danni si tiene conto in primo luogo dei danni per la popolazione e le sue basi vitali causati dal mancato funzionamento, da una perturbazione o dalla distruzione dell'infrastruttura critica. In particolare occorre tenere conto dei danni secondari (spesso difficilmente quantificabili) che risultano dall'interruzione del processo critico fino al suo ripristino. Molto importante è anche la disponibilità di ridondanze o alternative sufficienti per ovviare al servizio mancante (per es. trasporto su strada anziché su rotaia).

Dopo il rilevamento dell'entità dei danni si tratta di valutare la probabilità d'insorgenza o la plausibilità degli scenari. Dapprima si devono definire degli indicatori o delle classi idonee. L'appendice 3 riporta un esempio di indicatori e classi appropriati[12]. La scelta degli indicatori per stabilire la probabilità d'insorgenza deve essere documentata e motivata nel rapporto d'analisi. Con l'ausilio di questi indicatori si valuta infine la probabilità o la plausibilità del singolo scenario[13].

I valori relativi all'entità dei danni e alla probabilità d'insorgenza vengono in seguito inseriti nel compendio dei processi e delle minacce critiche. Per quanto riguarda gli indicatori per la valutazione dell'entità dei danni, si raccomanda di indicare sempre il valore della classe d'entità più elevata.

N°	Processo critico secondo il cap. 3.2.1	Risorsa rilevante secondo il cap. 3.2.2	Mancanza importante di risorse risp. minaccia per le risorse nella propria sfera di competenza	Rischio
1	Produzione	*Materie prime (esterno)*	*Penuria di materia prima*	E3 / P3
2	Produzione	Costruzioni/impianti (stabilimento X)	Terremoto	E5 / P5
3	Produzione	Costruzioni/impianti (stabilimento X)	Attentato convenzionale	E6 / P2
4	…	…	…	…
5	…	…	…	…

Tabella 6: Esempio di confronto tra processo critico, risorse e minacce (tabella 4) completato con la valutazione della probabilità d'insorgenza e dell'entità dei danni

I valori accertati possono infine essere rappresentanti in una matrice dei rischi. I diversi rischi sono così visibili a colpo d'occhio. La Figura 5 mostra un diagramma rischi-probabilità per i processi 1-3 (in alternativa o come complemento sull'asse delle ordinate può essere indicata anche la plausibilità).

[12] Per indicazioni supplementari sul metodo da seguire, cfr. «Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz», versione 1.03

[13] L'UFPP mette a disposizione le basi per la valutazione della plausibilità o della probabilità d'insorgenza e dell'evoluzione degli scenari.

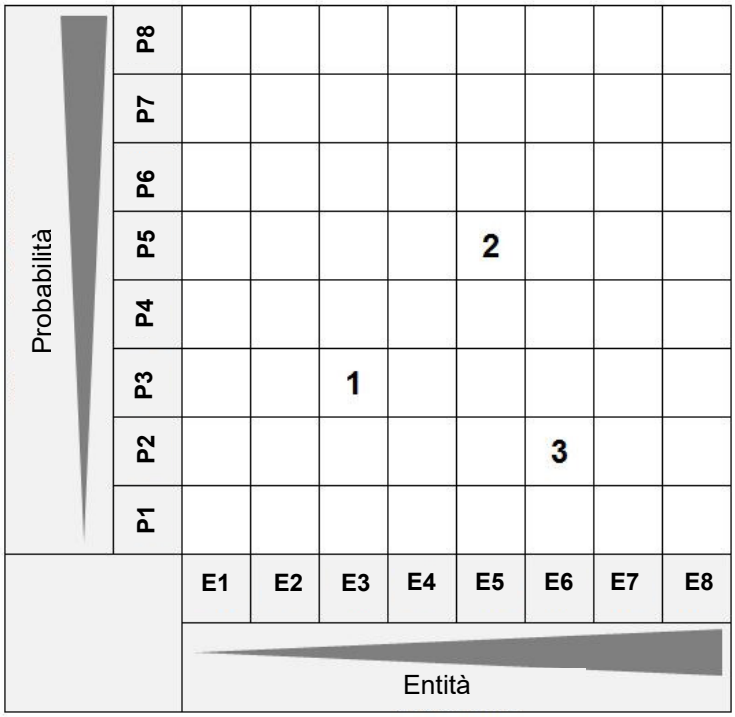


Figura 5: Esempio di matrice dei rischi

3.2.4 Stesura del rapporto d'analisi

Il rapporto d'analisi deve contenere tutte le informazioni importanti che sono emerse durante le fasi di preparazione e di analisi. La descrizione dello stato attuale deve limitarsi ai processi critici.

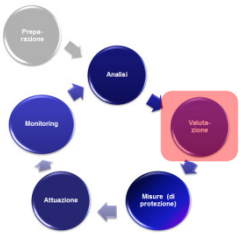
Se dall'analisi dovessero emergere gravi lacune concernenti la sicurezza dei processi critici (per es. *Single Point of Failure*, inosservanza di prescrizioni legali, ecc.), nel rapporto devono essere proposte anche le misure volte a colmare queste lacune in tempi brevi.

Il rapporto deve contenere essenzialmente i punti seguenti:

- breve descrizione del sistema
- indicazioni su precedenti lavori importanti in materia (basi RM e BCM)
- indicazioni relative ai processi critici
- indicazioni relative a risorse e punti vulnerabili importanti
- minacce rilevanti
  - indicatori rilevanti per l'entità di ogni singola minaccia compresa una breve motivazione per gli indicatori non rilevanti
  - entità e probabilità degli scenari
  - misure di sicurezza già implementate risp. già pianificate, di cui si è tenuto conto nell'analisi
- matrice dei rischi
- lacune individuate / misure urgenti necessarie (se già note)

Nel corso dei lavori successivi, il rapporto d'analisi deve essere completato con risultati relativi alle fasi di valutazione e di misure di protezione per infine ottenere il rapporto finale. L'appendice 6 riporta un esempio di struttura possibile. Il rapporto d'analisi copre i capitoli 1-3 del rapporto finale.

3.3 Valutazione



Al termine dell'analisi delle minacce e della vulnerabilità occorre stabilire quale livello di sicurezza perseguire. Ciò avviene nel quadro della fase di valutazione, dove sono rilevanti soprattutto gli obiettivi strategici che fra l'altro sono stati stabiliti nella strategia PIC nazionale (vedi anche il capitolo 1.2).

In relazione alla fase di valutazione, si tratta di rispondere alle domande seguenti:

- *Quanta sicurezza vogliamo?*
- *Che cosa siamo disposti a sacrificare in caso d'evento?*
- *Quanto siamo disposti ad investire per incrementare la sicurezza?*

In un primo tempo ci si orienta verso gli obiettivi strategici necessari per raggiungere il livello di sicurezza auspicato.

In base alla Strategia nazionale PIC il livello di sicurezza auspicato per le infrastrutture critiche è descritto nel modo seguente: la Svizzera garantisce la resilienza delle infrastrutture critiche in modo da evitare, nel limite del possibile, interruzioni importanti delle infrastrutture, dei beni e dei servizi e limitare l'entità dei danni in caso d'evento»[14].

Il livello di sicurezza definisce lo stato relativo alla sicurezza cui mirano tutti gli organi responsabili.

In relazione ai pericoli naturali, il livello di sicurezza consigliato dalla Piattaforma nazionale pericolo naturali (PLANAT) è il seguente: «il rischio... è così infimo che la sopravvivenza della comunità è garantita a oggi e per le generazioni successive. L'erogazione di beni e servizi di vitale importanza può essere interrotta in gran parte della Svizzera solo per un breve periodo»[15].

Dopo aver fissato gli obiettivi di protezione, si stabilisce il contributo concreto dei diversi responsabili al fine di raggiungere il livello di sicurezza auspicato.

Un obiettivo di protezione definisce il livello di sicurezza cui mirano determinati organi responsabili nella loro sfera di competenza.

In diversi ambiti della protezione delle infrastrutture critiche (per es. in singoli sottosettori o in relazione a singole minacce) gli obiettivi di protezione sono già stati fissati. Occorre assolutamente tenerne conto nell'applicazione della guida PIC. Occorre rispettare soprattutto gli obiettivi di protezione relativi ai rischi individuali (per es. rischio di morte).

La valutazione dei rischi collettivi (soprattutto dove **non** sono ancora stati definiti degli obiettivi di protezione) e le possibili misure nell'ambito della pianificazione volta a ridurre i rischi stessi, si fonda fra l'altro sul criterio dei costi marginali.[16] Questi rappresentano il limite della disponibilità di pagamento della collettività per impedire *un'*unità di danno (cioè quanto è disposta a pagare la collettività per impedire la morte di *una* persona, il danno economico di *un* franco, il danneggiamento di *una* determinata superficie dell'ambiente, ecc.).

[14] Strategia nazionale per la protezione delle infrastrutture critiche 2018 – 2022, FF 2018 467.
[15] Piattaforma nazionale Pericoli naturali (PLANAT), 2013: Livello di sicurezza per i pericoli naturali, agosto 2013, pag. 10
[16] Gli obiettivi di protezione assumono una funzione diversa secondo l'approccio scelto: nel campo dei pericoli naturali essi fungono ad esempio da criterio per la verifica delle necessità d'intervento. Una necessità d'intervento risulta in particolare quando vengono superati determinati valori limite in relazione al rischio complessivo o a singoli fattori del rischio (probabilità d'insorgenza o entità dei danni). L'approccio basato sui costi marginali applicato come complemento degli approcci esistenti, non prevede simili valori limite in relazione al rischio. La guida PIC è concepita in modo da essere compatibile con entrambi gli approcci.

3.3.1 Procedimento relativo alla valutazione dei rischi e delle vulnerabilità

Il procedimento concreto nell'ambito della fase di valutazione si suddivide in quattro passi:

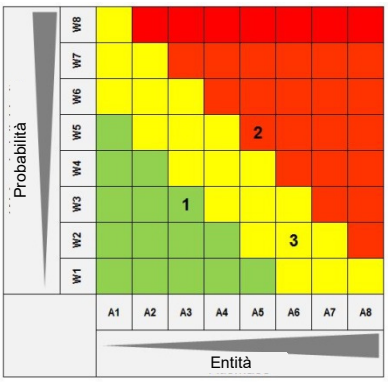
Primo passo: valutare tenendo conto delle direttive esistenti

Il punto di partenza è l'adempimento delle prescrizioni legali vigenti (*legal compliance*). Queste prescrizioni contemplano tutte le misure che un gestore IC è tenuto ad adottare per legge (rispetto di prescrizioni legali, norme, best practice, ecc.). Vi rientra inoltre l'adempimento di obiettivi di protezione più generali. Se, in relazione ai rischi analizzati, certe prescrizioni vigenti non sono adempiute, occorre immediatamente adottare provvedimenti per il loro adempimento (vedi capitolo 3.4).

Secondo passo: fissare le priorità dei rischi

In presenza di più scenari di minacce e processi critici, l'analisi dei rischi può condurre a un numero elevato di contributi. Di regola questi non rivestono però tutti la stessa importanza. Per semplificare la quantificazione dei rischi e la successiva pianificazione delle misure, in una prima fase è possibile effettuare un triage dei rischi secondo la loro importanza, oppure si possono formulare dei valori limite provvisori come obiettivo.

A tal fine, nella matrice dei rischi ogni rischio viene classificato secondo uno di tre livelli di priorità:



Priorità di pianificazione delle misure
rossa = elevata
gialla = media
verde = bassa

Figura 6: Proposta di classificazione secondo le priorità

Si può anche fissare un limite per sgravare la mole di lavoro, rinunciando a una successiva quantificazione dei rischi e alla pianificazione delle misure. La definizione dev'essere motivata e annotata nel verbale conclusivo.

Terzo passo: determinare i costi marginali rilevanti e l'avversione al rischio

Per poter quantificare i rischi, gli indicatori utilizzati per stabilire l'entità dei danni (cfr. capitolo 3.2.3) devono essere convertiti in un'unità monetaria. A tal fine si tratta tra l'altro di determinare la disponibilità della società ad evitare un'unità di danno.

Il punto di partenza è costituito da un indicatore guida per il quale sussistono le migliori basi, compreso il consenso per una monetizzazione (disponibilità di pagamento). Di regola si tratta di decessi, per i quali oggi esistono solide basi per una monetizzazione. Gli altri indicatori sono «calibrati» su questa base. Un esempio si trova nell'*appendice 4.1 – Proposte di costi marginali*.

Per tenere conto del fatto che la società cerca di evitare specialmente i rischi maggiori, è possibile determinare un fattore di avversione al rischio[17]. Un esempio di una funzione d'avversione si trova nell'*appendice 4.2 – Proposta di fattore d'avversione.*

I costi marginali e il fattore d'avversione vengono determinati d'intesa con le autorità specializzate competenti.

Al fine di garantire il confronto con altre analisi, si raccomanda di analizzare i rischi sia con, sia senza avversione.

Quarto passo: quantificare i rischi

Per i rischi definiti prioritari nella matrice dei rischi si procede a un'analisi quantitativa del rischio con l'ausilio degli indicatori dei danni monetizzati ed eventualmente della funzione di avversione. Per l'elaborazione ulteriore si raccomanda di convertire i rischi in un valore dei danni ipotizzati e di addizionarli per ogni processo o minaccia. Si ottiene così un compendio dei valori annui dei danni ipotizzati per ogni processo o tipologia di minaccia (vedi Figura 7). È inoltre possibile individuare il rischio complessivo risultante per le infrastrutture critiche (valore annuo dei danni ipotizzati).

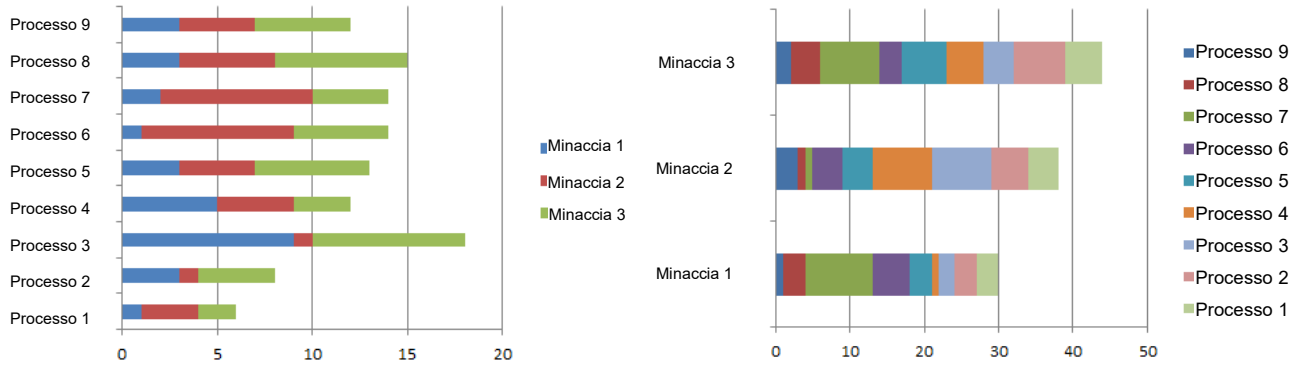
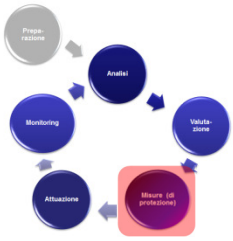


Figura 7: Compendio e struttura dei rischi per un esempio fittizio con 9 processi e 3 tipologie di minaccia. A sinistra: rischi correlati alle minacce per ogni processo; a destra: rischi correlati ai processi per ogni singola minaccia.

I rischi monetizzati costituiscono la base per la successiva pianificazione delle misure. In quest'ottica si tratta di verificare con quali misure e relativi costi è possibile ridurre i rischi a un livello accettabile. La decisione definitiva in merito all'attuazione delle misure (e quindi anche al livello concreto di sicurezza da raggiungere) viene presa una volta stabilita la combinazione ottimale delle misure. Nell'ambito di una ponderazione a livello politico occorre tenere conto anche di altri interessi (cfr. cap. 3.4.4). Il verbale allestito dopo la fase d'analisi dev'essere completato con i risultati della fase di valutazione. Occorre documentare in particolare quali costi marginali sono stati scelti per stabilire la disponibilità di finanziamento per i diversi indicatori.

[17] Un grande incidente stradale con 20 morti ha un impatto molto diverso sull'opinione pubblica che 20 piccoli incidenti con un solo morto nonostante il valore del rischio nei due casi sia lo stesso.

3.4 Misure (di protezione)



Nell'ambito della pianificazione delle misure si devono valutare le misure atte a ridurre i rischi identificati e analizzati in precedenza. Le domande fondamentali da porsi sono le seguenti:

- *Come si possono ridurre le conseguenze?*
- *Dove vi sono lacune (quali misure di protezione mancano)?*
- *Quali misure di protezione già esistenti devono essere completate o adattate?*
- *Quanto siamo disposti ad investire nelle misure volte ad incrementare la sicurezza?*

Il processo che permette di rispondere a queste domande è descritto nei seguenti sottocapitoli.

Fondamentalmente, in relazione ai rischi identificati si offrono tre opzioni: evitare i rischi, ridurre i rischi o trasferire i rischi. Dato che nel caso specifico delle infrastrutture critiche si tratta di funzioni d'importanza vitale per la società e l'economia, i cui rischi non possono essere completamente evitati né assicurati in modo adeguato, le seguenti spiegazioni si concentrano unicamente sugli aspetti della riduzione del rischio.

3.4.1 Sommario di tutte le possibili misure

In un primo passo si tratta di individuare tutte le possibili misure che permettono di ridurre i rischi accertati. Il ventaglio di misure prese in considerazione deve essere il più ampio possibile, per es.:

- misure edilizie (misure passive, schermatura del pericolo)
- misure tecniche (misure attive, «nel caso in cui»)
- misure nel campo del personale (indumenti e dispositivi di protezione, ecc.)
- misure di tipo organizzativo-amministrativo (direttive e divieti)
- misure nel campo del diritto (contratti, accordi sulle prestazioni, collaborazione in caso di catastrofe, ecc.)

Esempi di misure di protezione di questo tipo sono elencate nell'*Appendice 5 – Esempi di misure di protezione*. Questi esempi hanno unicamente carattere informativo e servono per completare eventuali misure di protezione già esistenti. Questo elenco non è esaustivo. Per ogni infrastruttura critica occorre chiarire quali misure esistono già e quali sono pianificate.

Considerato il costo elevato di talune misure, per la loro elaborazione si raccomanda di cercare la collaborazione con altri organi coinvolti. Potrebbe ad esempio essere sensato adottare delle misure sotto forma di soluzioni per settore (per es. un rafforzamento della collaborazione in caso d'evento, acquisizione di materiale di ricambio in comune, ecc.).

Occorre inoltre tener conto del fatto che nel caso di singole minacce d'intensità estrema potrebbe non essere sensato o possibile farvi fronte unicamente con misure alle infrastrutture critiche (per es. misure di protezione dell'oggetto). In questi casi occorre verificare con i servizi specializzati in minacce, risp. in misure (per es. uffici pericoli naturali o della protezione della popolazione) se è possibile adottare delle misure pubbliche presso la fonte di pericolo, risp. per lottare contro i pericoli.

I passi inerenti alla pianificazione e all'applicazione pratica delle misure qui di seguito descritti si riferiscono unicamente alle misure volte a rafforzare la resilienza delle infrastrutture critiche.

In relazione alle misure per il rafforzamento della resilienza delle infrastrutture critiche possiamo scegliere sia misure preventive che misure di preparazione. Nell'ambito della pianificazione delle misure occorre tener conto di entrambe le misure.

- **Misure di prevenzione**

  Si tratta di misure che permettono in primo luogo di ridurre la vulnerabilità di un'infrastruttura critica, vale a dire di evitare le minacce o perlomeno di ridurne le conseguenze. L'effetto delle misure di prevenzione si esplica prima che si verifichi l'evento.

- **Misure di preparazione**

  Si tratta di misure che permettono di ridurre i tempi d'interruzione di un'infrastruttura critica o di supportare la gestione di un evento al fine di limitare il più possibile l'entità dei danni. L'effetto delle misure di preparazione si esplica durante o dopo un evento.

  Occorre in particolare adottare misure volte a garantire la continuità operativa e la gestione delle emergenze e delle crisi, e completare i lavori in relazione ai risultati rilevati nei capitoli 3.2 e 3.3.

  Le basi per tali misure sono riportate nella tabella seguente:

Misure	Spiegazioni
Misure volte a garantire la continuità operativa	Nell'ambito della protezione delle infrastrutture critiche, la garanzia del funzionamento degli elementi infrastrutturali critici deve essere integrata in modo opportuno nei sistemi di *Business Continuity Management* (sistemi BCM) esistenti. A questo scopo può essere necessario adattare il BCM. Se all'interno dell'impresa non esistono misure volte a garantire la continuità operativa, queste devono essere pianificate e documentate nell'ambito del BCM. *Direttive e indicazioni su misure volte a garantire la continuità operativa si trovano ad esempio nei documenti seguenti:* *- ISO 22301: Societal Security – Business Continuity Management Systems – Requirements* *- ISO 22313: Societal Security – Business Continuity Management Systems – Guidance. First edition, 15 dicembre 2012.* *- Standard BSI 100-4 Gestione delle emergenze, Versione 1.0, 2008 (accento posto sull'IT-Service Continuity Management)* *- Quadro d'attuazione per la gestione delle emergenze secondo lo standard 100-4, 2013 (con accento sull'IT Service Continuity Management)* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- Guida BCM dell'Ufficio federale dell'approvvigionamento economico del Paese («Nessuna brutta sorpresa per la mia impresa»)* *- HB 221/2004 Business Continuity Management (in base a AS/NZS)*
Misure volte a gestire le emergenze	Le infrastrutture critiche devono essere adeguatamente integrate nella gestione interna delle emergenze. I concetti interni per l'allarme, l'allerta e l'evacuazione devono essere estesi alle infrastrutture critiche. Le misure immediate in caso d'emergenza per le infrastrutture critiche devono essere pianificate, preparate ed eventualmente adattate nell'ambito della gestione interna delle emergenze. Le organizzazioni d'emergenza devono essere istruite in materia di gestione delle emergenze presso infrastrutture critiche. Le misure immediate devono essere addestrate. In assenza di una gestione interna delle emergenze, questa deve essere istituita. *Per indicazioni e istruzioni relative all'istituzione di una gestione delle emergenze vedi per es.:* *- Standard BSI 100-4* *- ISO / PAS 22399*
Misure volte a gestire le crisi	Le infrastrutture critiche devono essere adeguatamente integrate nella gestione interna delle crisi. Quest'ultima deve essere istituita o adattata in modo tale che in caso di eventi che possono avere ripercussioni negative sul funzionamento di un'infrastruttura critica entri sempre in azione lo stato maggiore di crisi. In assenza di una gestione interna delle crisi, questa deve essere istituita. *Per indicazioni e istruzioni relative all'istituzione di una gestione delle crisi vedi per es.:*

	- Manuale di condotta operativa destinato ai membri degli organi civili di condotta (ed. Ufficio federale della protezione della popolazione, UFPP) *- British Standards Institute - PAS 200:2011 – Crisis management. Guidance and good practice* *- «Präventive Schadenbewältigung: Mehr gewinnen als verlieren», Schweizerische Rückversicherungsgesellschaft Swiss Re, 2001.* *- ISO 22320: Societal security – Emergency management – Requirements for incident response, 2011.*

Tabella 7: Settori in cui implementare le misure con indicazioni relative ai sussidi e alla letteratura in materia

3.4.2 Individuazione della combinazione economicamente ottimale delle misure

In un prossimo passo si tratta di stabilire, fra tutte le misure individuate, quali sono quelle costituenti la combinazione economicamente ottimale delle misure.

L'obiettivo è di raggiungere un rapporto ottimale tra i danni risultanti da interruzioni o perturbazioni delle IC e i costi necessari per l'attuazione pratica delle misure. La combinazione di misure ottimale è quella che implica i costi complessivi più bassi.

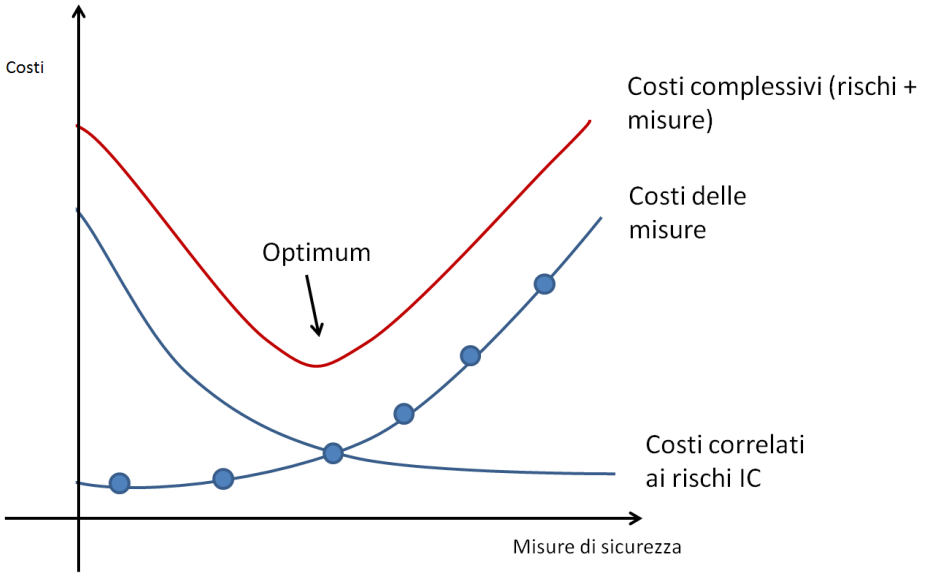


Figura 8: principio dei costi marginali; i punti blu rappresentano singole misure. Ogni misura implementata riduce i danni prevedibili in caso di interruzione o di perturbazione di un'IC. La combinazione ottimale di misure si trova dove i costi complessivi (vale a dire i costi per le misure e quelli generati dai danni conseguenti a interruzioni o perturbazioni alle IC) sono più bassi.

A questo scopo, partendo dall'elenco di tutte le possibili misure, viene data la priorità a quelle che presumibilmente presentano un rapporto costi-benefici positivo. Per queste vengono calcolati i costi annui dettagliati (costi d'investimento e costi ricorrenti). Si stima inoltre di quanto vengono ridotti i rischi grazie a queste misure. In seguito, tutte le misure atte a ridurre i rischi vengono elencate in ordine decrescente, secondo il rapporto tra riduzione del rischio e costi delle misure, e inserite in un grafico, dove sull'asse delle ordinate sono riportati i valori corrispondenti alla riduzione dei rischi e su quello delle ascisse i costi delle misure (vedi figura 9). Al poligono che ne risulta viene accostata una retta tangente con inclinazione -1 (criterio dei costi marginali). Nel punto di contatto, il criterio dei costi marginali è ancora soddisfatto. A destra di questo punto i costi delle misure di protezione superano quelli della potenziale riduzione dei danni. A sinistra dello stesso, i costi delle misure sono inferiori al danno che possono evitare.

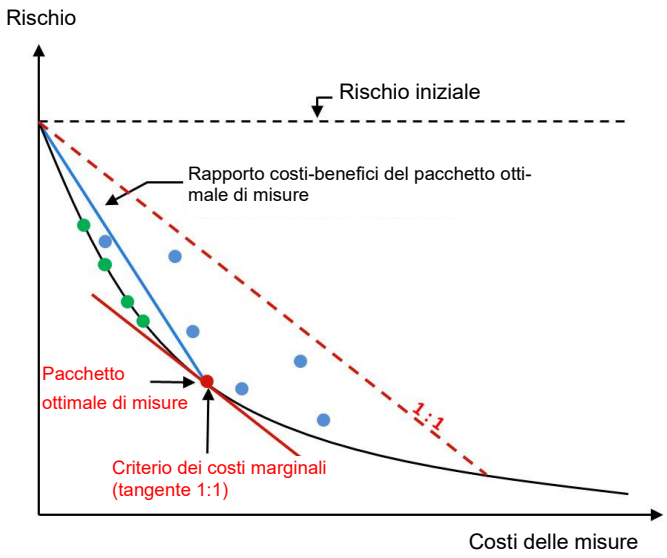


Figura 9: Procedimento per individuare la combinazione economicamente ottimale delle misure. La curva nera rappresenta il limite inferiore delle misure. Quelle che si trovano su di essa permettono di ottenere il massimo effetto (= riduzione del rischio) con un minimo di costi. Tutte le misure al di sotto della linea tratteggiata rossa (punti blu) presentano un rapporto utilità/costi superiore a 1, ma sono efficaci e ottimali solo se si trovano sulla curva nera fino al punto rosso della tangente = costi marginali (punti verdi).

Teoricamente è possibile che non venga trovata alcuna misura che presenti un rapporto costi-benefici positivo. Ciò può risiedere ad esempio nel fatto che non si sia pensato alle misure giuste durante la pianificazione. In questo caso è opportuno prendere in considerazione delle misure alternative per ridurre i rischi (vedi capitolo 3.4.1). Ma è anche possibile che per determinati rischi semplicemente non ci siano delle misure efficienti, anche dal punto di vista economico. In questo caso occorre elaborare delle strategie per gestire i rischi esistenti (vedi capitolo seguente).

3.4.3 Valutazione dei rischi residui e ponderazione globale degli interessi

Una volta individuata la combinazione di misure ideale con la ponderazione globale degli interessi, occorre valutarla in merito al rischio residuo. È particolarmente importante verificare se la combinazione di misure ottimale soddisfa tutte le condizioni poste (leggi, norme, direttive, prescrizioni in materia di obiettivi di protezione, ecc.). Se ciò non fosse il caso, si sceglierà la combinazione di misure più vicina a quella ottimale.

Come si evince dalla figura 9, una volta raggiunti i costi marginali rimane comunque un rischio (importante) al quale non è possibile far fronte con misure efficienti dal punto di vista economico. Dato che in caso d'evento questi rischi si concretizzano anche solo in parte sotto forma di danni effettivi, è importante aver elaborato già in precedenza una strategia per la loro gestione. Per i rischi aziendali si offre la possibilità dell'assicurazione, per i rischi rilevanti in ambito PIC è chiamato a intervenire lo Stato (per es. nell'ambito della prevenzione dei pericoli, mediante il sostegno sussidiario in caso d'evento, la creazione di un fondo di solidarietà, ecc.). Delle misure in tal senso vengono elaborate tra l'altro nell'ambito della strategia nazionale PIC.

Un grosso peso va inoltre attribuito alla comunicazione relativa ai rischi residui: un dialogo sui rischi fra tutte le parti interessate favorisce la consapevolezza generale, aumenta le conoscenze e sensibilizza la popolazione e l'economia interessata da questi rischi. Grazie a misure preventive individuali, in molti casi sono la popolazione e l'economia stesse a poter offrire un contributo efficace per la riduzione dei rischi.

Le misure non devono essere ottimali solo dal punto di vista economico, ma tenere conto anche di altri aspetti di sostenibilità globale. A tal fine occorre valutare quali conseguenze comporta la combinazione di misure proposta per i gestori interessati, l'ambiente, l'economia e la società.
Occorre anche chiarire come finanziare le misure. In particolare si deve garantire che non vi siano distorsioni della concorrenza o disparità di trattamento tra i gestori IC (anche per quanto riguarda la concorrenza internazionale). Dato che nell'ambito della protezione delle infrastrutture critiche l'accento è posto sulle prestazioni a favore della collettività, anche per quanto concerne il finanziamento delle misure occorre badare che si faccia partecipare la collettività alla riduzione dei rischi (per es. tramite fatturazione dei costi ai clienti o tramite la mano pubblica).

Occorre inoltre specificare come procedere per implementare le misure. Potrebbe essere necessario elaborare o completare le rispettive basi legali. Occorre quindi chiarire quali condizioni quadro devono essere soddisfatte a riguardo.

Se dalla ponderazione globale degli interessi risp. dalla valutazione dei rischi residui da parte delle autorità specializzate risultassero delle riserve nei confronti della combinazione di misure proposte, occorre effettuare gli accertamenti per le combinazioni di misure più vicine alla combinazione ottimale. Nell'impossibilità di stabilire delle misure che soddisfino le diverse esigenze della ponderazione globale degli interessi, occorre eventualmente verificare l'obiettivo strategico, risp le valutazioni effettuate (eventualmente obiettivi di protezione e costi limite, vedi capitolo 3.3).

3.4.4 Approvazione delle misure

I massimi organi direttivi (direzione aziendale, consiglio d'amministrazione, autorità specializzate, di vigilanza e di regolazione, governo cantonale, Consiglio federale, ecc.) devono decidere quali misure devono effettivamente essere realizzate tenendo conto anche di altri interessi (in particolare la sostenibilità ecologica, economica e sociale, la proporzionalità, il bisogno di sicurezza, ecc.). È senz'altro possibile che la quantità di sicurezza effettivamente realizzata sia maggiore o minore di quella definita come ottimale secondo il principio dei costi marginali.

Se per l'implementazione delle misure sono necessari degli adattamenti delle basi legali, la decisione finale delle misure da realizzare sarà presa a livello politico-sociale. Nell'ambito del processo legislativo c'è la possibilità che organi interessati (soprattutto le associazioni) possano avanzare le loro proposte (procedura di consultazione o d'audizione).

3.5 Attuazione delle misure

Di regola la responsabilità di pianificazione, realizzazione e controllo dell'attuazione delle misure compete ai gestori delle IC.

Se il budget o il personale non sono sufficienti per attuare tutte le misure contemporaneamente, si deve definire un ordine di attuazione. A questo scopo occorre tenere conto dei punti seguenti:

- Se un processo critico contiene un *single-point-of-failure*, ossia un punto che potrebbe portare al mancato funzionamento di tutti gli altri processi critici, questo dev'essere eliminato o reso sicuro con la massima priorità.
- Per tenere conto delle interdipendenze logiche, alcune misure devono essere necessariamente attuate in un certo ordine.
- Alcune misure hanno un effetto a largo raggio, altre un effetto piuttosto locale. Nell'ambito della protezione delle infrastrutture critiche è opportuno attuare dapprima quelle con effetto a largo raggio.

3.6 Monitoring, verifica e ottimizzazione delle misure

Al fine di migliorare costantemente la protezione delle infrastrutture critiche, oltre ad adottare misure adeguate e ad aggiornare costantemente la documentazione, occorre anche verificare regolarmente l'efficacia e l'efficienza della protezione integrale. A questo scopo l'organo direttivo interno competente dovrebbe effettuare regolarmente un controllo e una valutazione della protezione integrale (valutazione manageriale).

Tutti i risultati e le decisioni devono inoltre essere documentate in modo tracciabile. La verifica e l'ottimizzazione della protezione integrale concerne tutte le fasi, quindi sia i punti stabiliti nella fase di pianificazione preventiva e dell'attualità dei rischi esistenti, sia l'efficacia delle misure attuate e le misure preparatorie. Questi controlli dovrebbero avere luogo regolarmente, per es. annualmente. Delle verifiche supplementari sono necessarie in particolare

- dopo l'attuazione delle misure,
- dopo una situazione di crisi,
- dopo un ampliamento o una modifica dell'infrastruttura critica e
- in caso di cambiamento significativo della situazione di minaccia.

3.6.1 Esercitazioni / Test

Se determinati processi come ad esempio la messa in funzione e l'uso di installazioni tecniche vengono svolti solo sporadicamente, in caso d'evento non saranno svolti abbastanza rapidamente o addirittura in modo errato. Le strutture e le procedure delle diverse misure, in particolare quelle per eventi con bassa probabilità d'insorgenza ma grande entità di danni, devono quindi essere testate a intervalli regolari. Gli obiettivi sono[18]:

- verificare l'efficacia e la fattibilità delle misure,
- esercitare il coordinamento e la comunicazione in caso di crisi,
- testare i processi specifici in caso di crisi e perfezionarli in base alle esperienze pratiche,
- creare direttive per lo sviluppo delle strutture e delle procedure necessarie.

Occorre inoltre tenere conto del ritorno dall'esercizio d'emergenza all'esercizio normale.

Per lo svolgimento delle esercitazioni sono disponibili diversi tipi e metodi di esercitazione di vario grado d'astrazione e dispendio di mezzi[19].

3.6.2 Cura del processo PIC

Nell'ambito della protezione integrale, per ogni infrastruttura critica si devono sviluppare criteri di misurazione e di valutazione appropriati. Per poter seguire l'evoluzione occorre effettuare regolarmente delle misurazioni. In caso di evoluzione negativa, occorre individuare le cause, dedurre misure di miglioramento, designare i responsabili della loro attuazione e realizzare gli adattamenti.

[18] GUSTIN, Joseph F. Disaster & Recovery Planning: A Guide for Facility Managers, The Fairmont Press, Lilburn GA, 2004, p. 226.
[19] Direttive e istruzioni sui diversi tipi e metodi di esercitazione sono edite da: British Standards Institute – Published Document 25666:2010 – Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes.

3.6.3 Verifica

Solo grazie a verifiche periodiche della protezione integrale è possibile valutare se un'infrastruttura critica è in grado di far fronte a situazioni d'emergenza e di crisi. L'obiettivo è quello di garantire il funzionamento, l'efficacia, la proporzionalità e l'efficienza della protezione integrale. A tal fine occorre esporre i punti deboli e le possibilità di miglioramento nonché avanzare raccomandazioni.

La verifica della protezione integrale dovrebbe avvenire a vari livelli, per es. attraverso autovalutazioni, revisioni interne ed esterne. I controlli periodici ai diversi livelli devono essere pianificati, effettuati e in seguito documentati. Eventuali problemi individuati devono essere scadenzati e risolti.

Elenco delle abbreviazioni

Abbrevia-zione	*Spiegazione*
FF	Foglio federale
BCI	*The Business Continuity Institute* → www.thebci.org
BCM	*Business Continuity Management* → Spiegazione dei termini
BIA	Business Impact Analysis → Spiegazione dei termini
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik → https://www.bsi.bund.de
SCI	Sistema di controllo interno → Spiegazione dei termini
ISO	International Organization for Standardization → www.iso.org
IC	Infrastrutture critiche → Spiegazione dei termini
PIC	Protezione delle infrastrutture critiche → Spiegazione dei termini

Elenco delle figure

Elenco delle tabelle

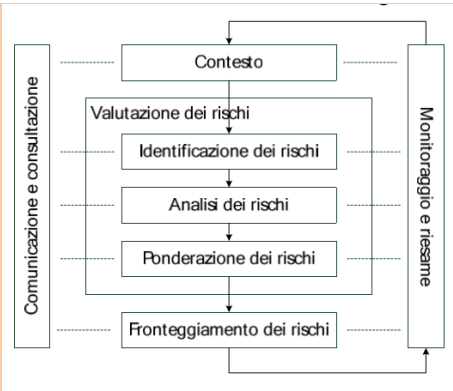
Spiegazione dei termini

Le seguenti definizioni rispecchiano il significato dei termini così come sono utilizzati nella guida PIC. Esse possono distanziarsi dall'uso che ne viene fatto in altre pubblicazioni. Con la freccia (→) si rimanda ad un'altra voce dell'elenco.

Termine	*Spiegazione*
Business Impact Analysis (BIA)	La *Business Impact Analysis* (it: analisi dell'impatto aziendale) consiste nell'analisi delle possibili conseguenze (finanziarie/materiali) di un incidente sull'attività aziendale. Si tratta di un procedimento per l'identificazione delle risorse critiche, delle esigenze per la ripresa della funzionalità e delle conseguenze di un'interruzione imprevista dell'attività. *Fonte (d): glossario BCMnet.CH, aprile 2013*
Business Continuity Management (BCM)	Il *Business Continuity Management* (it: continuità operativa) è un'attività di condotta olistica che permette di identificare i rischi (e le loro conseguenze sui processi aziendali), di pianificare le contromisure e di attuarle in caso d'evento. L'obiettivo è quello di mantenere possibilmente operativi i processi e le funzioni aziendali anche in caso di mancanza di risorse vitali per l'azienda. *Fonte (d): glossario BCMnet.CH, aprile 2013*
Probabilità d'insorgenza	Possibilità, stimata o basata su valori statistici, che un evento si verifichi in un determinato lasso di tempo (per es. ogni 10 anni).
Minaccia	Per minaccia s'intende un pericolo concreto che sussiste per un bene degno di protezione. La minaccia corrisponde quindi a un potenziale evento o a un potenziale sviluppo con possibili conseguenze per un bene degno di protezione. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Costi marginali	I costi marginali sono un metro di misura per la disponibilità a finanziare le misure volte a ridurre i rischi. Corrispondono concretamente ai costi massimi per unità di danni evitati che la società è disposta ad assumere per adottare misure volte a ridurre i rischi (→ rischio). *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Sistema di controllo interno (SCI)	Il sistema di controllo interno (SCI) è l'insieme di tutti i processi, metodi e provvedimenti di controllo che servono a garantire il buon svolgimento delle attività aziendali. Per le imprese di diritto privato, il sistema di controllo interno si fonda sul codice delle obbligazioni (art. 716a). Per l'Amministrazione federale, il sistema di controllo interno è descritto nella legge sulle finanze della Confederazione (LFC, art. 39) e nell'ordinanza sulle finanze della Confederazione (OFC, art. 36). Il SCI tratta i rischi (→ rischio) operativi nel campo dei rischi finanziari ed economici nonché i rischi giuridici (conformità alle regole vigenti, ossia «compliance»). *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Processo fondamentale	I processi fondamentali sono processi (→ processo) che contribuiscono direttamente all'adempimento del compito dell'infrastruttura critica come ad esempio l'adempimento di compiti statali trasmessi alle autorità, la prestazione di servizi o la fabbricazione di un prodotto.
Continuità operativa	Vedi: Business continuity management.
Efficacia dei costi	L'efficacia dei costi è un metro di misura che permette di valutare se i provvedimenti sono proporzionati. È quindi un parametro che mette a confronto l'→ efficacia delle misure (→ riduzione del rischio) con i costi generati. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*

Gestione di crisi	Preparazione sistematica alle situazioni di crisi e al loro fronteggiamento. La gestione di crisi comprende l'organizzazione di crisi, l'identificazione e l'analisi delle situazioni di crisi, lo sviluppo di strategie per affrontare le crisi nonché l'adozione e il monitoraggio costante delle contromisure. Implica sia la preparazione a situazioni di crisi, sia il coordinamento durante la crisi. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Infrastrutture critiche (IC)	Per «infrastrutture critiche» (IC) s'intendono processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della protezione.
Processo critico	Nell'ambito della protezione della infrastrutture critiche, per processo critico s'intende un processo indispensabile per il funzionamento dell'infrastruttura critica, la cui interruzione comporterebbe gravi conseguenze per la popolazione e le sue basi vitali.
Basi vitali	Le basi vitali sono l'insieme degli elementi di cui la popolazione ha bisogno per vivere. Esse rendono possibile la convivenza collettiva e individuale. Si possono suddividere in basi vitali naturali, economiche e sociali. - Basi vitali naturali: ambiente intatto (suolo, acque, aria, biodiversità) - Basi vitali economiche: economia florida e infrastrutture funzionanti - Basi vitali sociali: sistema giuridico funzionante, ordine costituzionale, fiducia reciproca, integrità territoriale e diversità culturale *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Gestione delle emergenze	La gestione delle emergenze (detta anche prevenzione delle emergenze) permette ad un'organizzazione di prepararsi a reagire rapidamente a una situazione straordinaria e a gestirla correttamente. Con la gestione delle emergenze vengono stabilite ed esercitate l'organizzazione in caso d'emergenza, le procedure d'allarme, la reazione schematica (misure immediate) a determinate situazioni d'emergenza, le istruzioni di comportamento ecc. e viene documentata la collaborazione con le organizzazioni di primo intervento. L'obiettivo è quello di non perdere tempo prezioso nel prendere decisioni, impartire ordini e assegnare competenze in caso d'emergenza. La gestione delle emergenze è focalizzata sull'obiettivo di salvare delle vite. Considerato che serve a gestire gli eventi, può essere considerata anche come parte del → Business Continuity Management (BCM) o della → gestione di crisi, poiché una situazione di crisi parte sempre da una situazione d'emergenza.
Processo	Un processo può essere visto come serie di (sotto)processi in cui si effettuano azioni e prese delle decisioni. Di regola ogni processo richiede input forniti da altri processi aziendali e fornisce risultati (output), ad esempio sotto forma di prodotti, informazioni o servizi. Gli input e gli output costituiscono il collegamento tra i diversi processi. A seconda del tipo, i processi aziendali vengono suddivisi in → processi fondamentali e → processi di sostegno.
Resilienza	La resilienza consiste nella capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni interne o esterne e di mantenere o ripristinare la capacità di funzionamento. La resilienza si compone di quattro elementi: 1) la robustezza dei sistemi (per es. → infrastrutture critiche, Stato, economia e società) di per sé; 2) la disponibilità di ridondanze; 3) la capacità di attivare misure di sostegno efficaci; 4) la tempestività e l'efficienza delle misure di sostegno. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*

Rischio	Il rischio è un metro di misura per le dimensioni di una minaccia e implica la → probabilità d'insorgenza e l'→ entità dei danni di un evento indesiderato. *Fonte: Glossario sui rischi, UFPP, 29.4.2013* Nell'ambito della protezione delle infrastrutture critiche, il termine «rischio» serve sia come modello per valutare gli aspetti legati alla sicurezza, sia per confrontare diversi → minacce tra loro in base agli stessi criteri. Il modello di rischio si fonda essenzialmente su due fattori: → la probabilità d'insorgenza di un evento; → l'entità dei danni per la popolazione e le sue → basi vitali. I rischi possono pertanto essere rappresentati come il prodotto tra la probabilità d'insorgenza di un evento e la sua entità dei danni.
Analisi dei rischi	L'analisi dei rischi rileva e descrive sistematicamente i rischi in un determinato sistema. Vi rientra la stima del livello dei rischi, spesso in forma di una classificazione degli scenari risp. della loro → probabilità d'insorgenza e dell'→ entità dei danni. L'analisi dei rischi cerca di rispondere alla domanda: «che cosa potrebbe succedere?». *Fonte: Glossario sui rischi, UFPP, 29.4.2013* L'analisi dei rischi è la base della → gestione dei rischi. Permette di descrivere → le caratteristiche del → rischio e a determinarne l'entità (ÖNORM ISO:3100). L'analisi dei rischi crea i presupposti possibilmente concreti e trasparenti per la pianificazione delle misure di protezione. In un primo passo vengono identificati ed elencati tutti i potenziali rischi che possono nuocere all'organizzazione. Per questi rischi vengono valutate le conseguenze (di regola di natura finanziaria) per il livello esaminato (per es. impresa o collettività) e la probabilità d'insorgenza. Le conseguenze e la probabilità d'insorgenza dei rischi dipendono dalla stima dell'intensità che sta alla base della valutazione. Occorre quindi elaborare degli scenari per i singoli rischi che permettano di effettuare tale stima. Per semplicità, di regola si prende in considerazione il «peggiore dei casi ancora plausibile» (*worst credible case*). L'entità del rischio corrisponde al prodotto tra entità dei danni e probabilità d'insorgenza. I risultati così ottenuti vengono infine rappresentati in una matrice dei rischi, che fungerà da base pianificatoria nell'ambito della → gestione dei rischi.
Gestione dei rischi	Per gestione dei rischi s'intendono le attività coordinate volte a gestire e condurre un'organizzazione in relazione ai rischi, vale a dire in relazione alle conseguenze delle incertezze sugli obiettivi dell'organizzazione. *Fonte: ÖNORM ISO 3100:2010* La gestione dei rischi è un processo sistematico per trattare in modo integrale i rischi. Si tratta di un processo consolidato nella società e nell'economia per il trattamento dei rischi. Essa viene strutturata e organizzata in modo diverso a seconda del contesto (elementi e ponderazioni). Il modello generale del processo di gestione dei rischi secondo lo standard ISO 3100 è raffigurato qui di seguito.

	 *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Riduzione dei rischi	Si distinguono due tipi di misure: quelle volte a ridurre la vulnerabilità degli elementi a rischio rispetto agli effetti di un pericolo, e quelle incentrate sulla continuità dei processi critici grazie alla creazione di ridondanze e soluzioni alternative. I sistemi ridondanti e quelli alternativi permettono la continuità operativa dei processi critici nell'ambito della gestione del ripristino della normalità, anche quando vengono compromessi degli elementi a rischio. *Fonte: Bundesministerium des Inneren, Schutz kritischer Infrastrukturen – Risiko-und Krisenmanagement – Leitfaden für Unternehmen und Behörden, Berlin, Januar 2008, S. 21-22.*
Scongiuramento dei rischi	I rischi possono essere scongiurati evitando le zone minacciate, oppure adottando misure volte a non generare minacce. Le zone minacciate sono quasi sempre identificabili vuoi perché sono esposte a pericoli naturali, o perché vicine ad impianti a rischio. Durante la pianificazione di nuove ubicazioni, edifici e impianti è quindi possibile evitare tali zone. Scongiurare del tutto i rischi è tuttavia impossibile, poiché nessun luogo è completamente esente da rischi. *Fonte: Bundesministerium des Inneren, Schutz kritischer Infrastrukturen – Risiko-und Krisenmanagement – Leitfaden für Unternehmen und Behörden, Berlin, Januar 2008, S. 21-22.*
Entità dei danni	Per entità dei danni s'intendono le conseguenze stimate per la popolazione e le sue → basi vitali provocate dal mancato funzionamento di uno o più → processi critici nel caso in cui la → minaccia dovesse concretizzarsi. Essa si compone della somma dei danni causati al momento del verificarsi dell'evento e di quelli che possono insorgere durante l'intera fase di ripristino.
Protezione delle infrastrutture critiche (PIC)	La protezione delle infrastrutture critiche comprende le misure atte a ridurre la → probabilità d'insorgenza e/o → l'entità dei danni di un guasto, un'interruzione o una distruzione di → infrastrutture critiche e quindi a minimizzare la durata della mancata disponibilità.
Obiettivo di protezione	Un obiettivo di protezione definisce il livello di sicurezza perseguito da determinati organi responsabili per il proprio ambito di competenza. *Fonte: Livello di sicurezza per i pericoli naturali, PLANAT 2013*
Interruzioni gravi	Un'interruzione è considerata grave quando nella zona in cui l'IC è rilevante (comune, cantone, regione, Paese, ecc.) dei beni e servizi importanti non sono disponibili per un periodo prolungato.
Gestione della sicurezza	Per gestione della sicurezza s'intendono la pianificazione, la conduzione e il controllo della sicurezza all'interno di un'organizzazione. Comprende aspetti della sicurezza dei sistemi tecnici ma anche aspetti non-tecnici, come ad esempio la sicurezza sul lavoro, la sicurezza d'esercizio e la sicurezza di locali e edifici. Viene spesso intesa come processo generale comprendente → la gestione dei rischi, il → Business Continuity Management (BCM), ecc. Esistono tuttavia anche forme organizzative in cui la gestione della sicurezza è integrata come misura nella → gestione dei rischi.

Livello di sicurezza perseguito	Stato di sicurezza a cui ambiscono tutti gli organi responsabili. *Fonte: Livello di sicurezza per i pericoli naturali, PLANAT 2013*
Single Point of Failure	Grave fonte di errore, che può causare l'interruzione completa dell'infrastruttura critica o dei suoi processi critici. Queste fonti di errore devono essere eliminate o rese sicure con la massima priorità.
Inventario PIC	L'Inventario PIC è un elenco degli oggetti IC la cui interruzione, perturbazione o distruzione potrebbe avere gravi conseguenze per la popolazione e le sue basi vitali. Si tratta da una parte di oggetti di grande importanza per l'approvvigionamento di beni o per la fornitura di prestazioni, e dall'altra di oggetti che rappresentano un grande potenziale di pericolo. Nell'Inventario sono riportati tra l'altro oggetti IC d'importanza nazionale. Esso sostituisce il catalogo SEE (salvaguardia delle esigenze esistenziali), tenuto all'epoca della difesa integrata. È stato realizzato sotto la direzione dell'Ufficio federale della protezione della popolazione (UFPP) in stretta collaborazione con gli organi responsabili della Confederazione e dei Cantoni e con i gestori IC e viene aggiornato regolarmente. Esso funge principalmente da base per i processi pianificatori e decisionali ai vari livelli (Confederazione, cantoni e gestori delle infrastrutture).
Processo di supporto	I processi di supporto non concorrono direttamente all'adempimento dei compiti di un'infrastruttura critica, ma possono svolgere indirettamente un ruolo importante e quindi critico, poiché servono a mantenere i → processi fondamentali. Nei processi di supporto di un oggetto IC possono rientrare ad esempio l'approvvigionamento di corrente elettrica e le telecomunicazioni.
Sottosettore	In Svizzera, le → infrastrutture critiche sono state suddivise in 28 sottosettori. Questi comprendono diverse categorie, come industrie, settori economici e altre suddivisioni di natura economica. Si tratta nella fattispecie dei sottosettori seguenti: acque di scarico, assicurazioni, approvvigionamento di petrolio, approvvigionamento idrico, banche, beni culturali, corrente elettrica, cure mediche e ospedaliere, derrate alimentari, gas naturale, industria elettro-meccanica e metallurgica, industrie chimiche e farmaceutiche, laboratori, organizzazioni di primo intervento, parlamento - governo - giustizia - amministrazione, media, rappresentanze diplomatiche e sedi di organizzazioni internazionali, ricerca e insegnamento, rifiuti, tecnologie dell'informazione, telecomunicazioni, traffico aereo, traffico postale, traffico ferroviario, traffico navale, traffico stradale e protezione civile.
Politica di sicurezza aziendale	Un elemento centrale dell'implementazione di una sicurezza aziendale integrale è la formulazione di una politica di sicurezza aziendale (ing. *Corporate Security Policy*). Nelle norme, negli standard e nella letteratura in materia si trovano definizioni molto diverse del termine «politica di sicurezza». Fondamentalmente essa definisce l'orientamento e la cultura di sicurezza nonché gli standard e le regole in materia di sicurezza all'interno di un'organizzazione. Dal momento che descrive il livello di sicurezza auspicato, si possono dedurre gli obiettivi di sicurezza per l'impresa (ISO/IEC TR 13335-1). La politica di sicurezza aziendale rispecchia la politica aziendale ed è generalmente emanata e convalidata dalla direzione. Nell'ambito della politica di sicurezza è la direzione ad assumersi la responsabilità della sicurezza aziendale (Müller, 2005). La politica di sicurezza aziendale deve essere pubblicata all'interno dell'impresa ed essere nota a tutti i collaboratori. Deve essere formulata in modo conciso, chiaro e comprensibile e limitarsi ad alcune pagine. Essa contempla tra l'altro gli aspetti seguenti: - importanza della sicurezza all'interno dell'impresa - riferimenti a disposizioni e leggi vigenti

	- obiettivi in materia di sicurezza ed elementi strategici necessari nonché metodi e standard da applicare - elementi dell'organizzazione di sicurezza - informazioni sulla verifica dell'attuazione della politica di sicurezza aziendale - informazioni sulle conseguenze dell'inosservanza della politica di sicurezza aziendale
Rischio residuo	Rischio che rimane dopo l'adozione di tutte le misure di sicurezza previste. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*
Efficacia	L'efficacia indica in che misura il → rischio viene ridotto grazie a un provvedimento. *Fonte: Glossario sui rischi, UFPP, 29.4.2013*

Appendice 1 – Basi metodologiche

Australia/Nuova Zelanda:

- AS/NZS 4360:2004 *Risk management* (replaced by AS/NZS ISO 31000:2009)
- HB 436:2004 *Risk Management Guidelines Companion to AS/NZS 4360:2004*
- AS/NZS 5050:2010 *Business Continuity – Managing Disruption Related Risks*
- HB 221:2004 *Business Continuity Management*

Germania:

- BBK: *Schutz kritischer Infrastruktur – Risikomanagement im Krankenhaus*, 2008
  http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungs-schutz/Band_2_Praxis_BS_Risikomanagm_Krankenh_Kritis.pdf?__blob=publicationFile
- BBK: *Methode für eine Risikoanalyse im Bevölkerungsschutz*, 2010
  http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd8_Methode-Risikoanalyse-BS.pdf;jsessionid =4914E21B99FB591B6EC2A0CCDBB766CD.1_cid345?__blob=publicationFile
- BMI: *Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement – Leitfaden für Unternehmen und Behörden*, 2. Auflage, 2011
  http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastruk-turen.html?nn=3314962
- BSI-Standard 100-4: *Notfallmanagement, Version 1.0, 2008 (Fokus auf IT-Service Continuity Management)*
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/stan-dard_1004_pdf.pdf?__blob=publicationFile
- *Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4*, 2013 (Fokus auf IT-Service Continuity Management)
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmen-werk/umra.html

Unione Europea:

- Commission Staff Working Paper SEC (2010) 1626 final: *Risk Assessment and Mapping Guidelines for Disaster Management*, 2010
  http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf
- European Network and Information Security Agency (ENISA): *Good Practice Guide for Incident Management*, 2010
  http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-manage-ment/at_download/fullReport

International Organization for Standardization (ISO):

- ISO/IEC 13335-1:2004: *Information Technology – Security Techniques -- Manage-ment of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Manage-ment*
- ISO 22301:2012 – *Societal Security – Business Continuity Management Systems – Requirements*
- ISO 22313:2012 – *Societal Security – Business Continuity Management Systems – Guidance. First edition, 15. December 2012*
- ISO 22320:2011 – *Sicherheit und Schutz der Gemeinwesens – Management der Gefahrenabwehr – Anforderungen an die Führungsstrukturen*, 2011
- ISO 22399:2007 – *Societal Security – Guideline for incident preparedness and op-erational continuity management*
- ISO/IEC 27001:2005 – *Information technology – Security Techniques – Information Security Management Systems – Requirements*
- ISO/IEC 27002:2005 – *Information Technology – Security Techniques – Code of Practice for Information Security Management*
- ISO 31000: 2009 – *Risk Management: Principles and Guidelines*

Austria:

- Austrian Standards Institute: *ONR 49000:2010 ff Risikomanagement für Organisationen und Systeme.* (Familie bestehend aus: ONR 49000, 49001, 49002-1, ONR 49002-2, 49002-3, 49003)

Svizzera:

- UFPP: *Analisi cantonale dei pericoli e preparazione alle situazioni d'emergenza. Guida KATAPLAN. Ottobre 2013*
  http://www.kataplan.ch
- UFPP: «*Analisi nazionale dei pericoli correlati a catastrofi e situazioni d'emergenza in Svizzera» – Rapporto sui rischi 2012*
  http://www.risk-ch.ch → Downloads
- UFPP: *Metodo di analisi dei rischi di catastrofi e situazioni d'emergenza in Svizzera (solo in tedesco: Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz),* versione 1.03, stato: 17 aprile 2013
  http://www.risk-ch.ch → Downloads
- UFPP: *Gestione integrale dei rischi. Importanza per la protezione della popolazione e delle sue basi vitali, 2014*
- UFPP: *Manuale di condotta operativa destinato ai membri degli organi civili di condotta*, documento 1300-00-5-i, 2010
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/it/home/dokumente/aubildungsunterlagen/fuehrungsbehelf_fuer.html
- UFPP / PLANAT: *Avversione al rischio: Entwicklung systematischer Instrumente zur Risiko- bzw. Sicherheitsbeurteilung – Rapporto riassuntivo (d/f)*, 2008
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/it/home/themen/gefaehrdungen-risiken/studien/risikoaversion.html
- UFPP: *Glossario dei rischi,* versione: 29 aprile 2013
- BCMnet.CH (Business Continuity Management Network Switzerland): *Glossario, Versione 1.1*, aprile 2013
  http://www.bcmnet.ch/downloads/Publikationen/BCMnet-Glossar-V1.1-1.4.14.pdf
- UFAE: *Guida BCM*: *Nessuna brutta sorpresa per la mia impresa,* n° d'ordinazione 750.142.i, novembre 2011
  http://www.bwl.admin.ch/dienstleistungen/01197/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXt9fGym162epYbg2c_JjKbNoKSn6A--
- AFF: *Handbuch zum Risikomanagement Bund,* versione del 29 aprile 2013
  http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf
- *GRF Davos: Obiettivi per la protezione delle infrastrutture critiche – Rapporto di base.* Mandato di ricerca n°. 353003897-SFA dell'Ufficio federale della protezione della popolazione, Berna. Settembre 2013
- *Strategia nazionale per la protezione delle infrastrutture critiche 2018 – 2022* (FF 2018 455-492)
  http://www.infraprotection.ch → Pubblicazioni PIC
- *Strategia nazionale per la protezione delle infrastrutture critiche* del 27 giugno 2012 (FF 2012 6875-6898)
  http://www.infraprotection.ch → Pubblicazioni PIC
- PLANAT: *Synthesebericht «Strategie Naturgefahren Schweiz»,* 2003
- PLANAT: *Piano di gestione dei rischi per pericoli naturali,* 2009
- PLANAT: *Livello di sicurezza per i pericoli naturali, agosto* 2013
- Associazione svizzera dei banchieri: *Raccomandazioni per il Business Continuity Management*, 2007
  http://shop.sba.ch/999925_i.pdf
- VBS: *Weisungen über die Massnahmen zur Aufrechterhaltung der Führungsfähigkeit des VBS (WBCM) vom 3. November 2011.*
- VBS/IOS: *Weisungen über das Integrale Schutzkonzept VBS (WISK, 94.102) vom 12. November 2012.*

- *Istruzioni sulla politica della Confederazione in materia di gestione dei rischi* del 24 settembre 2010 (FF 2010 5759).
  http://www.admin.ch/opc/it/federal-gazette/2010/5759.pdf

UK:

- Business Continuity Institute: *Good Practice Guidelines* – 2010
- British Standards Institute: BS 25999-1:2006 – *Business Continuity Management – Code of Practice*
- British Standards Institute: BS 25999-2:2007 – *Specification for Business Continuity Management*
- British Standards Institute: PAS 200:2011 – *Crisis Management. Guidance and Good Practice*
- British Standards Institute: BS 31100:2011 – *Risk Management – Code of Practice and Guidance for the Implementation of BS ISO 31000*
- British Standards Institute: Published Document 25666:2010 – *Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes*, 2010
- Center for the Protection of National Infrastructure: *Personnel Security Risk Assessment – A Guide,* 4th edition, 2013
  http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf?epslanguage=en-gb
- Center for the Protection of National Infrastructure: *Guide to Producing Operational Requirements for Security Measures*, 2013
  http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb
- Financial Services Authority (FSA): *Business Continuity Management Practice Guide,* 2006
  http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf
- The Institute of Risk Management: *A Risk Management Standard*, 2002

USA:

- American National Standard: ASIS SPC.1-2009 – *Organizational Resilience: Security Preparedness, and Continuity Management Systems-Requirement with Guidance for Use*, 2009
- National Fire Protection Association: NFPA 1600: *Standard on Disaster / Emergency Management and Business Continuity Programs*, 2010
- Department of Homeland Security: *National Infrastructure Protection Plan*, 2013
  https://www.dhs.gov/national-infrastructure-protection-plan

Altri autori ed editori:

- GUSTIN, Joseph F.: *Disaster & Recovery Planning: A Guide for Facility Managers*, The Fairmont Press, Lilburn GA, 2004
- PricewaterhouseCoopers AG: *Internes Kontrollsystem – Führungssystem im Wandel*, 2007
- Schweizerische Rückversicherungsgesellschaft Swiss Re: *«Präventive Schadenbewältigung: Mehr gewinnen als verlieren»*, 2001

Appendice 2 – Indicatori dei danni

I seguenti 12 indicatori dei danni sono ripresi dal metodo per l'analisi dei rischi correlati a catastrofi e situazioni d'emergenza in Svizzera (*Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz), versione 1.03*.

App. 2.1 – Decessi

Descrizione

Persone il cui decesso è da ricondurre direttamente all'evento o a una sua evoluzione.

E1	E2	E3	E4	E5	E6	E7	E8
0 – 1	2 – 3	4 – 10	11 – 30	31 – 1'00	101 – 3'00	301 – 1'000	> 1'000

App. 2.2 – Feriti/malati

Descrizione

Persone le cui ferite o patologie sono riconducibili all'evento o alla sua evoluzione. L'indicatore comprende tutte le forme di patologie e ferite psico-fisiche correlate alla minaccia. Si distinguono i seguenti livelli di gravità:

	Ferite	Patologie	Fattore
gravi	Ricovero in ospedale di almeno 7 giorni. Nessun danno fisico permanente.	Malattia cronica che necessita di cure mediche.	1
medie	Ricovero in ospedale da 1 a 6 giorni. Nessun danno fisico permanente.	Malattia grave di lunga durata che necessita di cure mediche; guarigione completa.	0.1
leggere	Nessun danno fisico permanente, cure mediche ma nessun ricovero in ospedale.	Malattia leggera che richiede cure mediche; guarigione completa.	0.003

I fattori di calcolo indicati permettono di tenere conto dei diversi livelli di gravità delle ferite.

E1	E2	E3	E4	E5	E6	E7	E8
≤ 10	101–30	31–100	101–300	301–1000	1001–3000	3001–10000	> 10'000

Le persone decedute in seguito a una patologia o alle ferite riportate non sono contemplate da questo indicatore, bensì dall'indicatore «decessi».

App. 2.3 – Persone bisognose d'aiuto

Descrizione

Questo indicatore include le persone che durante e/o dopo un evento devono essere evacuate, temporaneamente alloggiate e/o assistite in altro modo. Si tratta ad esempio di ospitare gli sfollati in alloggi di fortuna, di rifornire le persone rimaste isolate con derrate alimentari o di prestare un'assistenza psicologica a breve termine (aiuto psicologico d'urgenza) a persone che non soffrono di una vera e propria malattia fisica. Con l'indicatore viene rilevata la durata del bisogno di assistenza delle persone direttamente colpite. Le conseguenze, quali limitazioni e interruzioni nell'approvvigionamento di grandi fette di popolazione, sono rilevate dall'indicatore «Difficoltà e interruzioni d'approvvigionamento».

Il bisogno di sostegno è espresso nell'unità di misura «giorni per persone», vale a dire il prodotto tra il numero di persone bisognose d'aiuto e la durata delle prestazioni d'aiuto in giorni. È computata la durata effettiva del bisogno di aiuto per le persone colpite. La durata minima è di un giorno per persona. Viene rilevata la durata effettiva per la quale sussiste il bisogno di aiuto e non la durata per la quale vengono messe a disposizione le prestazioni di assistenza. Si conta ad esempio per quanti giorni le persone che hanno subito un trauma necessitano di aiuto psicologico, e non la quantità di giorni in cui i membri delle organizzazioni che prestano l'assistenza sono impiegate. I costi necessari per la prestazione di assistenza sono contemplati dall'indicatore «Danni patrimoniali e costi di gestione».

E1	E2	E3	E4	E5	E6	E7	E8
≤ 20'000	20'001–60'000	60'001–200'000	200'001–600'000.	600'001–2 Mio.	> 2–6 Mio.	> 6–20 Mio.	> 20 Mio.

App. 2.4 – Ecosistemi danneggiati

Descrizione

Questo indicatore rileva la superficie di territorio e/o di acque colpita da un effetto dannoso, per es. la fuoriuscita di sostanze velenose.

Un ecosistema è considerato danneggiato quando

a) l'equilibrio naturale è gravemente perturbato e i sistemi devono rigenerarsi:

e/o

b) importanti funzioni di un ecosistema sono limitate in modo importante (per es. quando le acque di superficie non sono più idonee ad essere utilizzate per l'approvvigionamento di acqua potabile).

I danni possono essere causati ad esempio da contaminazioni con sostanze chimiche o radiologiche, dalla colonizzazione di specie invasive (animali o vegetali) oppure da effetti fisici come ad esempio l'erosione.

I danni sono espressi nell'unità di misura «superficie all'anno» (km2 x anno), vale a dire il prodotto tra superficie colpita e numero di anni per i quali persiste il danno. Se una superficie è colpita da più effetti dannosi, questa viene rilevata una volta sola.

L'indicatore non tiene conto delle conseguenze dei danni agli ecosistemi (per es. limitazioni nell'approvvigionamento di beni e servizi vitali, come ad esempio difficoltà d'approvvigionamento di acqua potabile finché non è disponibile la logistica necessaria). Di queste conseguenze tiene conto l'indicatore G1 (Difficoltà e interruzioni d'approvvigionamento).

E1	E2	E3	E4	E5	E6	E7	E8
≤ 15	16–45	> 45–150	> 150–450	> 450–1500	> 1500–4500	> 4500–15'000	> 15'000

App. 2.5 – Danni patrimoniali e costi di gestione

Descrizione

L'indicatore «Danni patrimoniali e costi di gestione» misura i danni subiti dai valori patrimoniali e i costi sopportati per la gestione di un evento.

Il patrimonio si compone dei beni d'investimento e dei patrimoni finanziari. L'indicatore considera pertanto tutti i danni arrecati al patrimonio, indipendentemente dal fatto se sono risarciti da un'assicurazione, dallo Stato o da altri.

Nei costi di gestione rientrano ad esempio i costi del personale d'intervento, degli alloggi di fortuna e del vettovagliamento delle persone bisognose d'aiuto.

Esempio: un'inondazione causa danni a numerosi edifici e a un'industria. Sorgono costi per pompare l'acqua dalle cantine e ripulire il territorio dal fango e dai detriti (costi di gestione). Ma il danno materiale è un danno patrimoniale, poiché gli edifici e gli impianti hanno perso parte del loro valore.

A seconda delle conseguenze delle minacce, per la stima dei danni patrimoniali si può optare per uno dei seguenti due punti di vista:

• livello di economia globale: costi di gestione a livello nazionale e danni al patrimonio nazionale

• livello individuale o di territorio circoscritto: costi di gestione e danni patrimoniali per i singoli individui o un'unità geograficamente limitata.

E1	E2	E3	E4	E5	E6	E7	E8
≤ 5 Mio.	6–15 Mio.	> 15–50 Mio.	> 50 Mio.–150 Mio.	> 150 Mio. – 500 Mio.	> 500 Mio. – 1,5 Mrd.	> 1,5–5 Mrd.	> 5 Mrd.

App. 2.6 – Diminuzione dell'efficienza economica

Descrizione

L'indicatore dei danni considera le conseguenze economiche indirette che riducono il valore aggiunto in Svizzera.

Mentre l'indicatore «danni patrimoniali e costi di gestione» (cfr. app. 2.5) rileva i costi per la gestione e i danni arrecati al patrimonio, questo indicatore tiene conto delle conseguenze per la futura acquisizione di valore aggiunto.

Esempio inondazione (cfr. esempio nell'app. 2.5): a causa dei danni subiti, l'impresa toccata dall'inondazione deve sospendere la produzione per diverse settimane. Per questo subisce importanti perdite di reddito.

A seconda delle conseguenze delle minacce, per la stima dei danni patrimoniali si può optare per uno dei seguenti due punti di vista:

• livello di economia globale: come indicatore dell'efficienza economica viene utilizzata la somma del valore aggiunto in Svizzera. Questa somma viene quantificata nell'ambito del prodotto interno lordo (PIL). Una diminuzione dell'efficienza economica corrisponde pertanto a una riduzione del PIL.

• livello individuale o di territorio circoscritto: una diminuzione dell'efficienza economica delle persone colpite o in una determinata area.

E1	E2	E3	E4	E5	E6	E7	E8
≤ 5 Mio.	6–15 Mio.	> 15–50 Mio.	> 50 Mio.–150 Mio.	> 150 Mio. – 500 Mio.	> 500 Mio. – 1,5 Mrd.	> 1,5–5 Mrd.	> 5 Mrd.

App. 2.7 – Riduzione della qualità di vita

Descrizione

Questo indicatore permette di valutare la riduzione della qualità di vita per la popolazione in seguito a difficoltà o interruzioni nell'approvvigionamento (nota: le altre conseguenze di perturbazioni e interruzioni, per es. per l'economia, o conseguenti danni alle persone, sono contemplate da altri indicatori). Sono intese le interruzioni o gravi limitazioni nell'approvvigionamento dell'intera popolazione o di parti di essa con beni e servizi importanti. Questi vengono suddivisi in tre gruppi in base alla loro importanza.

Importanza	Beni	Servizi	Fattore
vitale	acqua potabile, alimenti di base, medicinali	cure mediche d'emergenza, comunicazione tra le forze d'intervento	1
molto importante	elettricità, energia per riscaldare, gas, abbigliamento, alloggi	cure mediche stazionarie e ambulatoriali (ad eccezione delle cure d'emergenza), cure ambulatoriali	0.3
importante	altre derrate alimentari, carburanti	telefono, IT, TV, traffico/trasporti (strada, rotaia, nave, ecc.)	0.1

Le limitazioni nell'approvvigionamento sono intese come il prodotto del numero di persone colpite e la durata delle limitazioni in giorni. Si computa la durata effettiva delle limitazioni per le persone colpite. Viene quindi rilevata la durata effettiva delle limitazioni, ossia, ad esempio, la durata complessiva dell'interruzione di corrente, vale a dire la somma dei singoli periodi d'interruzione, e non il numero di giorni in cui si sono verificate delle interruzioni di alcune ore.

Le conseguenze a livello economico sono rilevate dagli indicatori «Danni patrimoniali e costi di gestione» (app. 2.5) e «Diminuzione dell'efficienza economica» (app. 2.6). Eventuali altri danni per la popolazione sono inoltre valutati con gli indicatori «Decessi», «Feriti/malati» e «Persone bisognose d'aiuto» (cfr. app. 2.1-2.3).

E1	E2	E3	E4	E5	E6	E7	E8
≤ 50'000	> 50'000 – 150'000	> 150'000 – 0.5 Mio.	> 0.5 Mio. – 1.5 Mio.	> 1.5 Mio – 5 Mio.	> 5 Mio – 15 Mio.	> 15 Mio. – 50 Mio.	> 50 Mio.

App. 2.8 – Riduzione dell'ordine pubblico e della sicurezza interna

Descrizione

Questo indicatore rileva per quanto tempo e per quante persone che vivono in Svizzera sono limitati l'ordine la sicurezza. S'intendono nella fattispecie limitazioni in seguito a disordini interni che compromettono la vita quotidiana della popolazione. La limitazione è misurata in giorni per persone. La durata minima è di un giorno per persona.

E1	E2	E3	E4	E5	E6	E7	E8
≤ 10'000	> 10'000 – 30'000	> 30'000 – 100'000	> 100'000 - 300'000	> 300'000 - 1 Mio.	> 1 Mio. – 3 Mio.	> 3 Mio. – 10 Mio.	> 10 Mio.

App. 2.9 – Perdita di fiducia nello Stato e nelle istituzioni

Descrizione

L'indicatore funge da metro di misura della perdita di fiducia nello Stato e nelle sue istituzioni. Per istituzioni s'intendono organi esecutivi, legislativi e giudiziari nonché organizzazioni statali o cantonali come ad esempio amministrazioni, esercito e polizia. Ma vi rientrano anche le infrastrutture critiche, poiché la popolazione si aspetta che in Svizzera la disponibilità di beni e servizi essenziali come corrente, acqua, gas, ecc. non venga pregiudicata in modo grave.

L'entità della perdita di fiducia viene descritta in modo qualitativo.

E1	E2	E3	E4	E5	E6	E7	E8
Nessuna perdita di fiducia o perdita di fiducia della durata di pochi giorni correlata a temi poco rilevanti (per es. articoli critici nei media nazionali)	Perdita di fiducia di diversi giorni fino ad alcune settimane correlata a temi poco rilevanti (per es. articoli critici nei media nazionali)	Perdita di fiducia di pochi giorni correlata a temi di media importanza (per es. articoli molto critici nei media nazionali)	Perdita di fiducia di poche settimane correlata a temi di media importanza (per es. articoli molto critici nei media nazionali, dimostrazioni isolate)	Perdita di fiducia della durata di diverse settimane correlata a temi importanti (per es. articoli estremamente critici nei media nazionali; dimostrazioni isolate)	Perdita di fiducia della durata di alcune settimane correlata a temi importanti (per es. scioperi, dimostrazioni maggiori)	Perdita di fiducia della durata di diverse settimane correlata a temi importanti (per es. numerosi scioperi, dimostrazioni di massa)	Perdita importante della fiducia generale della durata di diverse settimane (per es. scioperi di lunga durata in diversi settori, dimostrazioni di massa in tutto il Paese)

App. 2.10 – Danni all'immagine del Paese

Descrizione

Questo indicatore rileva l'entità e la durata di un danno all'immagine del nostro Paese all'estero, vale a dire che il buon nome della Svizzera è compromesso e la Svizzera è messa in discussione come partner di accordi internazionali, bi- e multilaterali. L'indicatore tiene conto dell'entità e della durata del danno.

E1	E2	E3	E4	E5	E6	E7	E8
Danno d'immagine della durata di pochi giorni e correlato a temi poco rilevanti (per es. notizia diffusa in alcuni media esteri)	Danno d'immagine della durata di più giorni e correlato a temi poco rilevanti (per es. notizia diffusa in numerosi media esteri)	Danno d'immagine della durata di pochi giorni e correlato a temi di media importanza (per es. notizie negative diffuse in alcuni media esteri)	Danno d'immagine della durata di più giorni e correlato a temi di media importanza (per es. notizie negative diffuse in numerosi media esteri)	Danno d'immagine della durata di diversi giorni correlato a temi di media importanza (per es. notizie molto negative diffuse in alcuni media esteri)	Danno d'immagine della durata di una o più settimane correlato a temi di media importanza (per es. notizie molto negative diffuse in numerosi media esteri)	Danno d'immagine della durata diverse settimane (per es. notizie negative diffuse in praticamente tutti i media esteri rilevanti)	Grave danno d'immagine della durata di diverse settimane (per es. notizie molto negative diffuse in praticamente tutti i media esteri rilevanti)

App. 2.11 – Danneggiamento o perdita di beni culturali

Descrizione

Questo indicatore misura i danni o la perdita di beni culturali in Svizzera. I beni culturali degni di protezione comprendono beni mobili e immobili di grande importanza per il patrimonio culturale, quali ad esempio monumenti architettonici, artistici o storici, siti archeologici, libri, manoscritti, collezioni scientifiche, archivi o riproduzioni di tali beni. Vi rientrano anche edifici come musei, biblioteche, archivi, monasteri e i luoghi dove vengono custoditi i beni culturali mobili (cfr. Convenzione dell'Aia del 1954, art. 1).

Si distingue tra beni culturali d'importanza locale, regionale (oggetti B) e nazionale (oggetti A) e oggetti sotto «protezione rafforzata» (secondo la Commissione federale della protezione dei beni culturali).

Per «danneggiamento» s'intendono gravi interventi sui beni culturali, che ne causano la distruzione o che richiedono un grande onere finanziario e temporale per il restauro o la ricostruzione. Per «perdita» s'intende invece il furto e la distruzione irreversibile (per es. incendio, esplosione, inondazione).

E1	E2	E3	E4	E5	E6	E7	E8
Nessun danneggiamento o danneggiamento/perdita di singoli beni culturali d'importanza locale	Danneggiamento o perdita di diversi beni culturali d'importanza locale	Nessun danneggiamento o danneggiamento o perdita di singoli beni culturali d'importanza regionale	Danneggiamento o perdita di beni culturali d'importanza regionale e alcuni d'importanza nazionale	Danneggiamento o perdita di diversi beni culturali d'importanza regionale e alcuni d'importanza nazionale	Danneggiamento o perdita di diversi beni culturali d'importanza nazionale	Danneggiamento o perdita di numerosi beni culturali d'importanza nazionale	Danneggiamento o perdita di numerosi beni culturali d'importanza nazionale e di beni culturali sotto «protezione rafforzata»

Appendice 3 – Indicatori per la valutazione della probabilità d'insorgenza / plausibilità

Di seguito riportiamo un esempio di indicatori per la valutazione della probabilità d'insorgenza o della plausibilità degli scenari:[20]

Classe P	Descrizione	Probabilità	1 volta ogni . . . anni	Frequenza (1/anno)
P 8	In Svizzera lo scenario si verifica in media poche volte nella durata di vita di una persona.	> 30 %	< 30	> $3*10^{-2}$
P 7	In Svizzera lo scenario si verifica in media una volta nella durata di vita di una persona.	10 - 30 %	30 - 100	$3*10^{-2}$ - 10^{-2}
P 6	Lo scenario si è già verificato in Svizzera, ma può risalire a diverse generazioni passate.	3 - 10 %	100 - 300	10^{-2} - $3*10^{-3}$
P 5	Forse lo scenario non si è ancora verificato in Svizzera, ma è noto da altri Paesi.	1 - 3 %	300 - 1'000	$3*10^{-3}$ - 10^{-3}
P 4	Si conoscono diversi di questi scenari a livello mondiale.	0.3 - 1 %	1'000 - 3'000	10^{-3} - $3*10^{-4}$
P 3	Si conoscono alcuni di questi scenari a livello mondiale.	0.1 - 0.3 %	3'000 - 10'000	$3*10^{-4}$ - 10^{-4}
P 2	Si conoscono solo pochi di questi scenari a livello mondiale, ma potrebbero verificarsi anche in Svizzera.	0.03 - 0.1 %	10'000 - 30'000	10^{-4} - $3*10^{-5}$
P 1	Se si sono verificati, si conoscono solo rarissimi casi di questo scenario a livello mondiale. Ciononostante non si può del tutto escludere che si verifichi in Svizzera.	< 0.03%	> 30'000	< $3*10^{-5}$

Esempio di indicatori per la valutazione della probabilità d'insorgenza

Secondo la nomenclatura di cui sopra, la frequenza definisce il numero di eventi (previsti) per unità di tempo. *La frequenza è solitamente espressa in numero di eventi l'anno (per es. numero di valanghe in Svizzera in un anno).*

Probabilità

La probabilità si riferisce a un possibile evento. Si tratta di definire qual è la probabilità che un determinato evento si verifichi. La probabilità è un valore compreso tra 0 e 1, ma può essere espressa anche con un valore tra 0 e 100%.

La frequenza definisce pertanto il numero (previsto) di eventi in un certo intervallo di tempo, mentre la probabilità descrive la possibile occorrenza di un determinato evento quando le condizioni per la sua insorgenza sono date nel caso specifico.

Nel caso di minacce naturali e tecnologici, la probabilità o la frequenza con cui uno scenario di minaccia si verifica viene calcolata in modo possibilmente preciso, ad esempio sulla base di statistiche o di valutazioni di esperti quando non sono disponibili dati sufficienti.

Plausibilità

Agli eventi provocati intenzionalmente (per es. eventi politici, attentati terroristici o conflitti armati) non è sempre possibile associare una frequenza o una probabilità d'insorgenza precisa poiché la situazione di minaccia può mutare rapidamente. Per questo tipo di minaccia si può

[20] Questa scala si basa sul metodo e sui lavori di *«Catastrofi e situazioni d'emergenza in Svizzera»* (2013).

stimare la plausibilità dell'insorgenza (per es. nel corso dei prossimi dieci anni) (tabella 3).

Analogamente alle classi di probabilità e di frequenza, agli scenari di minaccia può essere associata anche una classe di plausibilità[21].

[21] Vedi: Katastrophen und Notlagen Schweiz – Methode zur Risikoanalyse, Versione 1.03, 17 aprile 2013, pag. 8 (tabella 3: Klassen für Plausibilität).

Appendice 4 – Costi marginali e fattore d'avversione

App 4.1 – Proposte di costi marginali

Indicatore	Costi marginali per unità di misura
Decessi	CHF 4 mio.
Feriti/malati	CHF 400'000
Persone bisognose d'aiuto	CHF 250
Ecosistemi danneggiati	CHF 11'500
Danni patrimoniali e costi di gestione	CHF 1
Diminuzione dell'efficienza economica	CHF 1
Riduzione della qualità di vita	CHF 500
Riduzione dell'ordine pubblico e della sicurezza interna	CHF 300
Perdita di fiducia nello Stato e nelle istituzioni	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mia. / A7: 3.25 Mia. / A8: 10 Mia.
Danni all'immagine del Paese	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mia. / A7: 3.25 Mia. / A8: 10 Mia.
Danneggiamento o perdita di beni culturali	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mia. / A7: 3.25 Mia. / A8: 10 Mia.

Fonte: Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz. Versione 1.03, Stato 17 aprile 2013 - tabella 5, pag. 23.

App. 4.2 – Proposta di fattore d'avversione

Nel 2008, uno studio congiunto dell'UFPP e di PLANAT ha proposto un fattore di avversione φ comprendente i tre effetti derivanti dalla crescente incertezza:

- φ1: incertezza nella valutazione della probabilità d'insorgenza
- φ2: incertezza nella valutazione dei danni
- φ3: incertezza nell'atteggiamento intrinseco nei confronti del rischio

Per l'applicazione pratica, i tre fattori vengono definiti singolarmente, ma poi di nuovo riuniti in un unico fattore φ.

Quantificazione del fattore d'avversione φ

In un primo passo sono stati stimati i fattori φ1 e φ2 per l'incertezza nella valutazione della probabilità d'insorgenza w e dell'entità dei danni E, tenendo conto di un intervallo di confidenza del 95% (ca. 2σ). I due fattori φ1 e φ2 sono poi stati sommati per ottenere un unico fattore φ1+2, i cui valori sono riportati nella seguente tabella:

Numero di decessi	1	10	100	1'000	10'000	100'000	1'000'000
Probabilità d'insorgenza all'anno Jahr	5.0 E+00	1.1 E-01	6.2 E-03	2.8 E-04	1.8 E-05	2.4 E-06	5.0 E-07
Fattore φ1+2	1.0	1.25	1.5	1.8	2.15	2.5	2.9

Successivamente si stima il fattore φ3, che corrisponde all'avversione in senso stretto. Non è possibile rispondere in modo oggettivo alla domanda: in che misura la società deve tenere conto di questo effetto. Teoricamente questa decisione dovrebbe essere ad esempio presa da una fetta rappresentativa e ben informata della popolazione, intesa come surrogato dell'opinione pubblica. Visto che un procedimento di questo tipo è molto oneroso e complesso da attuare, nell'ambito dello studio sull'avversione ai rischi del 2008 sono stati fissati i valori seguenti:

Numero di decessi	1	10	100	1'000	10'000	100'000	1'000'000
Fattore φ 3	1.0	1.3	1.8	2.5	3.2	3.8	4.0

I fattori φ1+2 e φ3 sono stati combinati tramite la seguente formula:

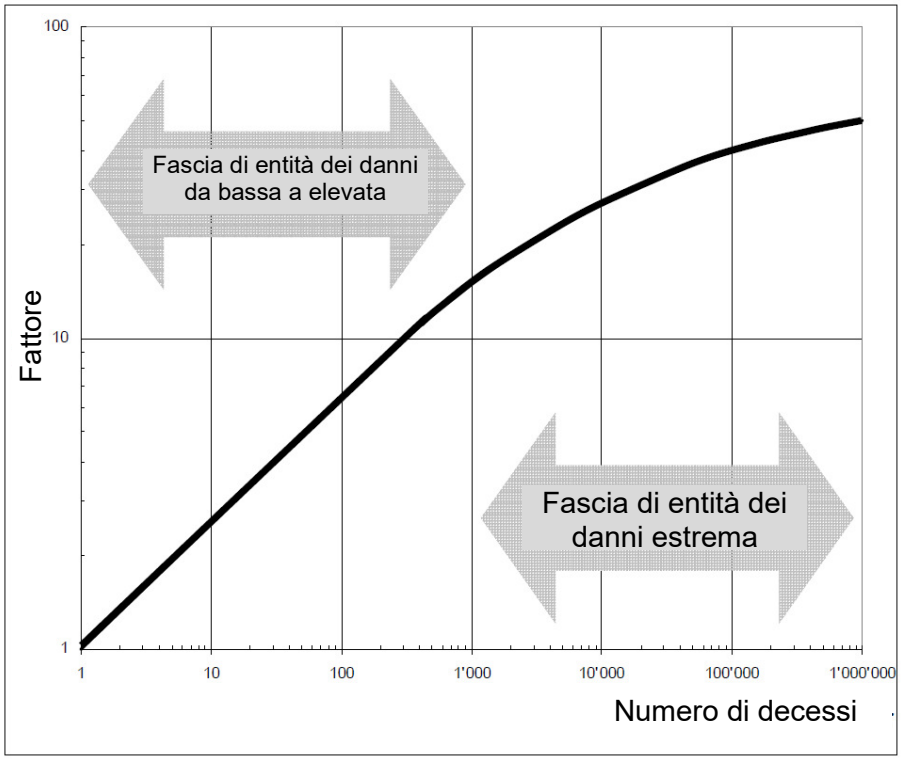
$$R_m = \sum_i w_i \cdot A_i \cdot f_i \cdot \varphi_i \cdot GK$$

wobei:

i	indice degli scenari
R_m:	rischio monetizzato di tutti gli scenari i
w_i :	probabilità d'insorgenza [/anno]
A_i :	entità dei danni [decessi]
f_i:	fattore complementare dei danni
φ_i	fattore d'avversione
GK:	costi marginali

L'effetto cumulativo di questi fattori è rappresentato nella figura seguente.

I singoli fattori sono inoltre stati riuniti in un fattore globale che può essere comparato con fattori d'avversione già esistenti. A questo scopo l'entità dei danni E è stata suddivisa in due fasce: entità dei danni da bassa a elevata (fino ad un massimo di mille decessi) e entità dei danni estrema (da mille a un milione di decessi).



Fonte: UFPP/PLANAT: Risikoaversion. Entwicklung systematischer Instrumente zur Risiko- bzw. Sicherheitsbeurteilung. Zusammenfassende Bericht / Aversion pour le risque. Développement d'instruments systématiques pour l'évaluation du risque et de la sécurité . Rapport de synthèse *(testo disponibile solo in tedesco / francese)*. Berna, 2008, pag. 15-17

Appendice 5 – Esempi di misure di protezione

App. 5.1 – Esempi di misure di natura tecnico-edilizia

Misure di protezione tecnico-edilizie

Ubicazione dell'oggetto

- Protezione da pericoli naturali (inondazioni, terremoti, onde di tempesta, frane e colate di fango, valanghe, tempeste, ecc.)
- Distanze dagli edifici vicini
- Evitare costruzioni chiuse (accesso da tetti vicini, ecc. reso più difficoltoso)
- Protezione contro i pericoli tecnologici (incidenti in centrali nucleari, incidenti chimici, ecc.)

Tipo di costruzione

- Accessi stradali (uscite d'emergenza)
- Protezione contro le effrazioni
- Posizione degli edifici degni di protezione
- Facciate lisce (senza sporgenze)
- Nessuna possibilità d'appiglio per arrampicarsi sulle facciate
- Condotte e allacciamenti sotterranei (non manipolabili)
- Prese esterne disattivabili

Provvedimenti antintrusione

- Recinzione (completa, antintrusione, altezza minima, antiscavalcamento (filo spinato), contro il sottopassaggio, videosorveglianza)
- Porte e cancelli antintrusione
- Controlli d'accesso elettronici (citofoni, videosorveglianza, sistema a chiusa, lettori di tessere d'identità, codici numerici, ecc.)
- Detezione elettronica automatica (allarmi su recinzioni e cancelli, videotecnica con sensori,
- Illuminazione esterna (se possibile senza zone d'ombra e non manipolabile)
- Personale per il controllo dei mezzi di detezione elettronica
- Personale di guardia istruito, in grado di intervenire ed equipaggiato (per es. con telecamere termiche/a raggi infrarossi)
- Messa a dimora di piante ≠ possibilità di superare le misure di natura tecnico-edilizia

Sistemi di sicurezza negli edifici

- Protezione visiva per i settori sensibili
- Rinunciare ad indicazioni sull'ubicazione dei settori sensibili
- Settori di sicurezza separati
- Protezione dei settori di sicurezza separati (elettronica, meccanica, controlli d'accesso, sorveglianza speciale)
- Sensore antintrusione su porte, finestre, lucernari e pozzi di luce
- Finestre con griglie
- Protezione dei lucernari e dei pozzi di luce (griglie di copertura solide, chiusure anti-sollevamento)
- Protezione dei pozzi di alimentazione e di scarico (griglie)
- Protezione (griglie) di finestre spesso aperte (per es. nei WC)
- Vetri di sicurezza nei settori di sicurezza speciali
- Protezione delle finestre (serramenti antintrusione, vetri infrangibili, maniglie con chiavistello, listelli fermavetro avvitati)
- Numero limitato di porte d'accesso
- Protezione dell'entrata principale (lettore di carta o chip d'identificazione, serrature autochiudenti, apriporta di sicurezza elettrici, chiudiporta automatici, citofono con telecamera, chiusa, entrata e uscita separate)
- Protezione delle uscite di sicurezza (serrature automatiche, chiudiporta automatici, allarme sulle porte)
- Consegna di chiavi solo a persone autorizzate
- Custodia sicura delle chiavi di riserva
- Amministrazione delle autorizzazioni

Protezione antincendio

- Parafulmini
- Rispetto delle prescrizioni antincendio
- Pianificazione ed esercitazioni antincendio
- Impianto di segnalazione dei pericoli sempre presenziato

… ecc. …

App. 5.2 – Esempi di misure di natura organizzativo-amministrativa

Misure di protezione organizzativo-amministrative

Interne all'azienda

- Incaricato della sicurezza
- Personale addetto alla sicurezza interno all'azienda (conoscenza delle basi legali necessarie per lo svolgimento dei loro compiti, degli obblighi e dei diritti correlati al loro compito e alla loro applicazione pratica)
- Chiarezza in merito alle prescrizioni e/o alle norme legali in materia di sicurezza
- Regolamentare le esigenze legate alla sicurezza (per es. tramite direttive, linee guida, ecc.)
- Protocollare gli eventi rilevanti per la sicurezza
- Trarre insegnamenti da eventi rilevanti per la sicurezza
- Conoscenze del personale in relazione alla protezione sul lavoro, alla protezione antincendio e ai primi soccorsi
- Identificare potenziali pericoli e indicatori di preallerta
- Inventario di processi, oggetti, sistemi ed elementi critici
- Catasto delle sostanze pericolose
- Piani di tutte le condotte di alimentazione e di scarico (per es. elettricità, acqua, gas, telefono, ecc.)
- Piani per le diverse situazioni di minaccia
- Strategia per incidenti che pregiudicano la sicurezza
- Piano d'allarme
- Regole di comportamento e iter di notifica in caso di incidenti che pregiudicano la sicurezza
- Informazioni sulle vie di fuga
- Esercitazioni d'evacuazione
- Esercitazioni «Rimanere sul posto» (per es. in caso di incidente nelle vicinanze)
- Esercitazioni antincendio
- Integrare gli insegnamenti tratti dalle esercitazioni di addestramento
- Comunicazione in caso di crisi
- Assistenza psicologica durante incidenti rilevanti per la sicurezza

Esterne all'azienda

- Collegamenti d'emergenza per le telecomunicazioni
- Gestione indipendente della sicurezza integrale (ossia in mano unicamente all'azienda)
- Accordi tra l'azienda e i fornitori di servizi nel campo della sicurezza (struttura del contratto, collaborazione pratica, competenze in caso di crisi)
- Introduzione/formazione continua del personale addetto alla sicurezza
- Analisi della criticità per l'outsourcing di servizi
- Nessuna disponibilità open source (per es. immagini aeree dell'azienda in Internet, ecc.)

… ecc. …

App. 5.3 – Esempi di misure nel campo del personale

Misure di protezione nel campo del personale

Personale (interno ed esterno)

- Controllo di sicurezza dei collaboratori (interni ed esterni)
- Obbligo del personale a rispettare leggi, prescrizioni, obblighi contrattuali, disposizioni interne, ecc.
- Sensibilizzazione del personale sulle questioni inerenti la sicurezza (corsi, esercitazioni, seminari, team training, ecc.)
- Reclutamento (esperienza, conoscenze, controllo del background [estratto del casellario giudiziario, ecc.], integrità, controllo delle referenze)
- Partenze (restituzione di documenti, materiale d'ufficio, chiavi, password, badge, ecc., non-disclosure agreement, ecc.)
- Protezione dei quadri (protezione della persona, ecc.)

Estranei

- Obbligo d'annuncio; registrazione dell'arrivo e della partenza nel giornale dei visitatori
- Rapida identificazione dei visitatori (per es. tramite cartellini)
- Accompagnamento/sorveglianza dei visitatori
- Controllo dei fornitori e delle merci

… ecc. …

App. 5.4 – Esempi di misure di natura organizzativa e giuridica

Misure di protezione organizzative e giuridiche

Contratti e Service Level Agreements in relazione a

- Stoccaggio di mezzi d'esercizio supplementari in altre località;
- Accordi con fornitori di prestazioni esterni per la fornitura in tempi brevissimi dei mezzi necessari all'esercizio;
- Deviazione concordata di forniture just-in-time verso altre località;
- Stoccaggio di mezzi necessari all'esercizio in depositi o luoghi d'imbarco sicuri;
- Trasferimento di determinati segmenti della produzione in altre località che dispongono dei mezzi d'esercizio necessari;
- Accordi sull'utilizzo di mezzi d'esercizio alternativi;
- Intese contrattuali per le situazioni d'emergenza.

… ecc. …

App. 5.5 – Esempi di misure volte a garantire la continuità operativa

Misure a favore della continuità operativa

Disponibilità di personale con funzioni chiave
È importante sviluppare strategie adeguate per preservare conoscenze e capacità importanti per l'azienda:
- documentazione sullo svolgimento di processi e attività critiche;
- multi-skil-training per collaboratori e fornitori di prestazioni importanti;
- condivisione delle competenze trasversali al fine di evitare un'inutile concentrazione dei rischi;
- coinvolgimento di terze persone;
- pianificazione regolamentata delle successioni;
- salvaguardia e gestione delle conoscenze.

Disponibilità di ubicazioni o di locali alternativi per garantire la continuità operativa
Occorre una strategia chiara volta a ridurre le conseguenze in caso di mancata disponibilità di una sede o di determinati locali:
- locali o sedi/località separate all'interno dell'azienda;
- locali o sedi/località esterne all'azienda (per es. presso aziende partner, ecc.)
- locali separati o sedi/località presso fornitori di prestazioni esterni;
- postazioni di home-office e accesso remoto;
- risorse di personale alternative in altri locali o sedi/località.

Ripristino del funzionamento tecnico e disponibilità di alternative (in particolare TIC)
La scelta della strategia dipende in larga misura dal tipo di tecnologie utilizzate nell'azienda:
- distribuzione geografica di mezzi e installazioni tecniche;
- disponibilità di mezzi/installazioni tecniche di riserva/sostitutive.

Si tratta inoltre di scegliere strategie specifiche anche per le tecnologie dell'informazione:
- identificare e definire il Recovery Time Objective (RTO), soprattutto per quelle attività e quei processi definiti critici;
- distribuzione geografica e distanza tra le ubicazioni tecnologiche;
- quantità di ubicazioni tecnologiche;
- accesso remoto;
- ricorso a ubicazioni non presenziate;
- collegamenti di telecomunicazione e allacciamenti ridondanti;
- tipo di «failover»: avvio manuale o automatico dei sistemi ridondanti;
- collegamenti tramite fornitori terzi.

Salvaguardia/ripristino delle informazioni
Le informazioni essenziali per il funzionamento dell'oggetto IC devono essere protette e ripristinabili (nel lasso di tempo stabilito nell'analisi). Informazioni supplementari su questo tema si trovano nello standard ISO/IEC 27001.

Ogni informazione necessaria per il funzionamento di processi e/o oggetti critici, deve soddisfare le caratteristiche seguenti.
- confidenzialità;
- integrità;
- disponibilità;
- attualità (validità);
- copie fisiche;
- copie elettroniche.

Garanzia della disponibilità di prestazioni di servizio esterne
Ogni azienda dovrebbe allestire un elenco dei mezzi d'esercizio importanti per i processi e gli oggetti critici. A questo scopo deve tenere conto dei punti seguenti:
- stoccaggio di mezzi d'esercizio supplementari in un'altra località;
- accordi con fornitori di prestazioni esterni per la fornitura, in tempi ristretti, dei mezzi d'esercizio necessari;
- deviazione concordata di forniture just-in-time verso altre località;
- stoccaggio di mezzi d'esercizio in luoghi d'imbarco sicuri;
- trasferimento di determinati segmenti della produzione in altre località che dispongono dei mezzi d'esercizio necessari;
- ricerca di mezzi d'esercizio alternativi;
- incremento del numero di fornitori (per ridurre la dipendenza da un singolo fornitore)
- promozione di strategie BCM presso i fornitori;
- accordi contrattuali per le situazioni d'emergenza;
- ricerca di fornitori alternativi.

… ecc. …

Appendice 6 – Concetto di protezione integrale. Esempio di struttura per un rapporto finale

Ricapitolazione

1. **Introduzione**
   - Contesto
   - Obiettivi del rapporto
   - Organi coinvolti

2. **Basi e lavori preesistenti**
   - Basi generali
   - Basi legali rilevanti
   - Lavori preesistenti rilevanti

3. **Analisi**
   - Descrizione dell'infrastruttura critica
   - Determinazione dei processi critici
   - Identificazione delle risorse e dei punti vulnerabili rilevanti
   - Analisi dei rischi
   - Eventuali misure urgenti

4. **Valutazione**
   - Valutazione tenuto conto delle direttive esistenti
   - Definizione delle priorità per i rischi
   - Determinazione dei costi marginali e dell'avversione
   - Quantificazione dei rischi / compendio dei rischi

5. **Misure (di protezione)**
   - Compendio delle possibili misure
   - Scelta delle misure prioritarie e accertamento dei costi
   - Identificazione della combinazione ottimale di misure
   - Ponderazione globale degli interessi
   - Implementazione delle misure (necessità di adattare/creare il quadro legislativo)
   - Raccomandazioni per l'attuazione (competenze, procedimento), verifica e aggiornamento
   - Determinazione del reporting e della verifica dei progressi nell'attuazione delle misure

6. **Procedimento ulteriore**
   - Proposte per il procedimento ulteriore

Allegati
- Documentazione dei processi critici
- Elenco degli esperti e degli organi specializzati contattati

Appendice 7 – Settori e sottosettori critici

Settori	Sottosettori
Autorità	Ricerca e insegnamento
	Beni culturali
	Parlamento, governo, giustizia, amministrazione
Energia	Approvvigionamento di gas naturale
	Approvvigionamento di petrolio
	Approvvigionamento d'energia elettrica
	Teleriscaldamento e calore di processo
Smaltimento	Rifiuti
	Acque di scarico
Finanze	Servizi finanziari
	Servizi assicurativi
Sanità pubblica	Prestazioni mediche
	Servizi di laboratorio
	Chimica e agenti terapeutici
Informazione e comunicazione	Servizi informatici
	Telecomunicazioni
	Media
	Servizi postali
Alimentazione	Approvvigionamento alimentare
	Approvvigionamento idrico
Sicurezza pubblica	Esercito
	Organizzazioni di primo intervento (polizia, pompieri, sanità)
	Protezione civile
Trasporti	Traffico aereo
	Traffico ferroviario
	Traffico navale
	Traffico stradale

Fonte: Strategia nazionale per la protezione delle infrastrutture critiche 2018-2022, FF 2018 455.

Appendice 8 – Organi federali con mansioni di coordinamento

Settore	Sottosettore	Organi federali competenti (elenco non esaustivo)*
Autorità	Ricerca e insegnamento	DEFR (SEFRI)
	Beni culturali	DDPS (UFPP), DFI (UFC)
	Parlamento, governo, giustizia, amministrazione	Servizi del Parlamento, CaF, DFAE, DFI (MeteoSvizzera) DFGP (fedpol) DDPS (SIO, SIC), DFF (AFF, ODIC e LE), DATEC (UFAM)
Energia	Approvvigionamento di gas	DATEC (UFE, IFO), DEFR (UFAE)
	Approvvigionamento di petrolio	DATEC (UFE, IFO), DEFR (UFAE)
	Approvvigionamento di elettricità	DATEC (UFE, ELCOM, ESTI, IFSN, DEFR (UFAE)
	Teleriscaldamento e calore di processo	DATEC (UFE)
Smaltimento	Rifiuti	DATEC (UFAM)
	Acque discarico	DATEC (UFAM)
Finanze	Servizi finanziari	DFF (FINMA, AFF, SFI), DEFR (UFAE), DATEC (UFCOM)
	Servizi assicurativi	DFF (FINMA, AFF, SFI), DFI (UFAS)
Sanità pubblica	Assistenza medica	DDPS (SSC), DFI (UFSP), DEFR
	Servizi di laboratorio	DFI (UFSP, USAV), DDPS (UFPP)
	Prodotti chimici e agenti terapeutici	DEFR (UFAE), DFI (Swissmedic), DDPS (Aggruppamento Difesa)
Informazione e comunicazione.	Servizi informatici	DEFR (UFAE), AFF (ODIC)
	Telecomunicazioni	DATEC (UFCOM), DEFR (UFAE)
	Media	DATEC (UFCOM)
	Servizi postali	DATEC (UFCOM), DEFR (UFAE)
Alimentazione	Approvvigionamento alimentare	DEFR (UFAE, UFAG)
	Approvvigionamento idrico	DATEC (UFAM), DEFR (UFAE)

Settore	Sottosettore	Organi federali competenti (elenco non esaustivo)*
Sicurezza pubblica	Esercito	DDPS (Aggruppamento Difesa)
	Organizzazioni di primo intervento (polizia, pompieri, sanità)	DFGP (fedpol), DDPS (UFPP)
	Protezione civile	DDPS (UFPP)
Trasporti	Traffico aereo	DATEC (UFAC), DEFR (UFAE)
	Traffico ferroviario	DATEC (UFT), DEFR (UFAE)
	Traffico navale	DATEC (UFT), DEFR (UFAE)
	Traffico stradale	DATEC (USTRA), DEFR (UFAE)

* Gli organi citati determinano assieme al Segretariato PIC quali altri organi (Confederazione, Cantoni, associazioni, ecc.) dirigono o devono essere coinvolti nel rafforzamento della resilienza. Le competenze vigenti vengono mantenute.

Abbreviazioni degli organi federali competenti

USTRA	Ufficio federale delle strade
UFPP	Ufficio federale della protezione della popolazione
UFAM	Ufficio federale dell'ambiente
UFSP	Ufficio federale della sanità pubblica
UFC	Ufficio federale della cultura
UFCOM	Ufficio federale delle comunicazioni
UFT	Ufficio federale dei trasporti
UFAC	Ufficio federale dell'aviazione civile
UFCL	Ufficio federale delle costruzioni e della logistica
UFE	Ufficio federale dell'energia
UFAG	Ufficio federale dell'agricoltura
UFAS	Ufficio federale delle assicurazioni sociali
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
DFAE	Dipartimento federale degli affari esteri
AFF	Amministrazione federale delle finanze
ElCom	Commissione federale dell'energia elettrica
IFSN	Ispettorato federale della sicurezza nucleare
IFO	Ispettorato federale degli oleo- e gasdotti
ESTI	Ispettorato federale degli impianti a corrente forte
fedpol	Ufficio federale di polizia
FINMA	Autorità federale di vigilanza sui mercati finanziari
SG DATEC	Segreteria generale del DATEC
PIO	Protezione delle informazioni e delle opere (Stato maggiore dell'Esercito, DDPS)
ODIC	Organo di direzione informatica della Confederazione
SSC	Servizio sanitario coordinato
SIC	Servizio delle attività informative della Confederazione
SFI	Segreteria di Stato per le questioni finanziarie internazionali

DATEC	Dipartimento federale dell’ambiente, dei trasporti, dell’energia e delle comunicazioni
SEFRI	Segreteria di Stato per la formazione, la ricerca e l’innovazione
BNS	Banca nazionale svizzera
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport