

Strategia nazionale per la protezione delle infrastrutture critiche

del 27 giugno 2012

Riassunto

Le infrastrutture critiche garantiscono la disponibilità di beni e servizi vitali come l'approvvigionamento energetico, le comunicazioni o il traffico. Interruzioni su vasta scala hanno gravi ripercussioni sulla popolazione e sull'economia e compromettono la sicurezza e il benessere dello Stato.

Nei singoli settori critici la Svizzera dispone di un elevato grado di sicurezza e gode di un contesto relativamente stabile, così che finora le perturbazioni gravi sono state sporadiche e di breve durata. Ma a pari passo con la tecnologizzazione e con la globalizzazione è cresciuta anche l'importanza delle infrastrutture critiche: un blackout generalizzato dell'approvvigionamento di corrente metterebbe a terra l'intera economia del Paese, causerebbe interruzioni anche nell'ambito delle altre infrastrutture critiche (p. es. telecomunicazioni, approvvigionamento idrico o traffico ferroviario) e comporterebbe gravi disagi per la popolazione (mancato funzionamento di illuminazione, sistemi di refrigerazione, riscaldamenti, ascensori ecc.). Inoltre le catastrofi naturali, che si manifestano con sempre maggiore frequenza, gli attacchi cibernetici e l'invecchiamento dei sistemi tecnici hanno fatto sì che negli ultimi anni i rischi per le infrastrutture siano cambiati. Le forti interdipendenze in caso d'evento richiedono infine una collaborazione sempre più stretta di tutti gli attori coinvolti.

Per questi motivi è necessario, tramite la presente strategia nazionale, rafforzare in modo significativo la resilienza (capacità di resistenza) della Svizzera in relazione alle infrastrutture critiche. A questo scopo la strategia definisce diverse misure suddivise in due campi d'azione. Nel campo delle infrastrutture critiche viene migliorata l'autoprotezione grazie all'allestimento e all'applicazione, da parte degli organi competenti, di piani di protezione integrali volti a identificare e ridurre i rischi specifici. A livello intersettoriale viene migliorata la collaborazione fra gli organi coinvolti (autorità, gestori) di tutti i settori delle infrastrutture critiche e ridotta la vulnerabilità della società, dell'economia e dello Stato in vista di interruzioni gravi. In questo senso vengono elaborate pianificazioni volte a limitare i danni e a sostenere in modo sussidiario i gestori in caso di interruzioni gravi. Sono inoltre contemplate misure quali l'allerta tempestiva in caso d'evento o il rafforzamento dell'autoprevenzione da parte della popolazione e dell'economia in vista di simili interruzioni.

Nell'ambito della protezione delle infrastrutture critiche sono diversi i progetti, le misure ecc. importanti che devono essere presi in considerazione. La strategia nazionale «protezione delle infrastrutture critiche» si applica principalmente nel quadro delle strutture e delle competenze esistenti. Sono fatte salve le competenze degli organi federali coinvolti.

Strategia nazionale

1 Introduzione

La Svizzera dipende da una fitta rete di infrastrutture critiche il cui funzionamento deve essere garantito in ogni momento. Queste permettono infatti la disponibilità di beni e servizi importanti come l'approvvigionamento energetico, le comunicazioni o i trasporti. L'interruzione di infrastrutture critiche si ripercuote negativamente sull'economia e sulla popolazione e compromette la sicurezza e il benessere dello Stato. La protezione delle infrastrutture critiche (PIC) è pertanto un compito centrale dello Stato e delle imprese.

La necessità di proteggere le infrastrutture critiche non è nuova. In singoli settori o in vista di pericoli o contromisure specifiche gli organi competenti di Confederazione, Cantoni e gestori si occupano già ora di aspetti della protezione di infrastrutture critiche che contribuiscono a raggiungere l'obiettivo comune. Sono per contro mancati per molto tempo un coordinamento intersettoriale e un modo di procedere concertato e globale nei diversi settori.

Per questo motivo il Consiglio federale ha incaricato l'Ufficio federale della protezione della popolazione (UFPP) di coordinare le attività in questo campo e di elaborare, entro la primavera 2012, una strategia nazionale PIC.

La strategia nazionale PIC fissa gli obiettivi perseguiti dalla Svizzera in questo ambito e illustra i provvedimenti necessari per ridurre i rischi per le infrastrutture critiche. Essa contribuisce pertanto alla protezione della popolazione, alla salvaguardia del benessere economico e alla sicurezza del Paese.

La strategia delinea il campo d'applicazione, definisce le infrastrutture critiche e fissa principi generali per la protezione delle infrastrutture critiche. Fornisce inoltre un quadro dello stato attuale dei lavori nel campo della protezione delle infrastrutture critiche in Svizzera e all'estero. Illustra gli obiettivi e cita 16 misure attribuite a due campi d'azione distinti. Spiega infine in quali strutture e con quali competenze viene attuata la strategia.

La strategia nazionale PIC si rivolge a tutti gli organi con competenze nell'ambito della protezione delle infrastrutture critiche, in particolare alle autorità competenti (Confederazione, Cantoni e Comuni), alle autorità politiche e ai gestori delle infrastrutture critiche.

2 Campo d'applicazione e definizione di infrastrutture critiche

Il campo d'applicazione della strategia nazionale per la protezione delle infrastrutture critiche è dato dalla definizione dei termini rilevanti e dalla catalogazione delle infrastrutture critiche.

Infrastrutture

L'iperonimo «infrastrutture» comprende le installazioni e le organizzazioni che forniscono prodotti e servizi a favore della società, dell'economia e dello Stato.

Infrastrutture critiche

Le infrastrutture critiche sono quelle il cui mancato funzionamento a causa di perturbazioni, guasti o distruzione hanno gravi ripercussioni sulla società, sull'economia e sullo Stato. Le infrastrutture critiche sono suddivise in tre livelli:

- *settori*: p. es. energia, finanze, sanità pubblica
- *sottosettori*: p. es. approvvigionamento di energia elettrica, approvvigionamento di petrolio, approvvigionamento di gas naturale
- *oggetti/elementi (singoli)*: p. es. centrali e sistemi di comando, centri di calcolo, dighe, condotte, aziende operatrici

Lo spettro delle infrastrutture critiche è il seguente:

Tabella 1

Elenco delle infrastrutture critiche

Settori	Sottosettori
Autorità	Rappresentanze diplomatiche e sedi di organizzazioni internazionali
	Ricerca e insegnamento
	Beni culturali
	Parlamento, governo, giustizia, amministrazione
Energia	Approvvigionamento di gas naturale
	Approvvigionamento di petrolio
	Approvvigionamento di energia elettrica
Smaltimento	Rifiuti
	Acque di scarico
Finanze	Banche
	Assicurazioni
Sanità pubblica	Cure mediche e ospedaliere
	Laboratori
Industria	Industrie chimiche e farmaceutiche
	Industrie elettro-meccaniche e metallurgiche
Informazione e comunicazione	Tecnologie dell'informazione
	Media
	Traffico postale
	Telecomunicazioni
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
	Criticità molto elevata*
	Criticità elevata*
	Criticità normale*
<p>* – Per criticità s'intende l'importanza relativa del sottosettore in relazione a fattori quali la popolazione, l'economia e le dipendenze (≠ significato assoluto). Per la deduzione di eventuali misure si deve inoltre tenere conto della situazione concreta di minaccia e della vulnerabilità delle infrastrutture.</p> <p>– Nella ponderazione non si fa riferimento alla criticità di singoli oggetti.</p> <p>– La ponderazione si basa su una situazione di pericolo normale.</p>	

Protezione delle infrastrutture critiche

La protezione delle infrastrutture critiche comprende le misure atte a ridurre la probabilità e/o l'entità dei danni di un guasto, un'interruzione o una distruzione di infrastrutture critiche e quindi di minimizzare la durata della non disponibilità.

3 Principi per la protezione delle infrastrutture critiche

Approccio globale basato sui rischi: la protezione delle infrastrutture critiche si fonda sui rischi esistenti. Il rischio risulta dalla minaccia, dalla criticità e dalla vulnerabilità delle infrastrutture. Nell'analisi dei pericoli si tiene conto di uno spettro molto ampio. Ciò significa che fondamentalmente si tiene conto di tutti i pericoli rilevanti (pericoli naturali, pericoli tecnologici e pericoli sociali)¹. Anche lo spettro delle misure da valutare deve essere possibilmente completo (aspetti edilizi, tecnici, organizzativi e giuridici per le fasi: prevenzione, mitigazione, gestione di situazioni di crisi e d'emergenza, ripristino e ricostruzione). Deve inoltre essere garantita anche la protezione delle informazioni.

Proporzionalità: i costi per l'attuazione delle misure di protezione delle infrastrutture critiche devono essere proporzionali alla loro utilità. Le misure scelte devono inoltre essere costituzionali e legittimate sul piano giuridico. Sono infine da evitare inutili distorsioni del mercato.

Responsabilità propria: i provvedimenti devono essere adottati sia dal settore pubblico, sia dai gestori delle infrastrutture critiche. Dato che la maggior parte delle infrastrutture critiche è gestita da imprese private, il miglioramento autonomo delle misure di protezione è di grande importanza. Le autorità competenti sono invitate a verificare se ciò sia sufficiente o se sia eventualmente necessario fissare obiettivi a livello politico.

Collaborazione tra pubblico e privato: la protezione delle infrastrutture critiche richiede una maggiore collaborazione tra tutti gli organi coinvolti (autorità a livello federale, cantonale e comunale e i gestori di infrastrutture critiche). Dove possibile le misure di protezione devono essere elaborate e applicate congiuntamente. La collaborazione tra settore pubblico e privato deve essere verificata in tutti i settori della protezione delle infrastrutture critiche, in particolare nell'ambito dei progetti edilizi (p. es. la nuova costruzione di infrastrutture critiche), della redazione di norme e direttive e in relazione allo scambio di informazioni.

¹ I pericoli sono catalogati conformemente al progetto «Rischi Svizzera».

4

Stato attuale

4.1

La protezione delle infrastrutture critiche in Svizzera

La situazione nel campo delle infrastrutture critiche in Svizzera è illustrata qui di seguito.

- Esiste già un gran numero di organizzazioni, strutture, misure, regolamentazioni, progetti ecc. che contribuiscono alla protezione delle infrastrutture critiche.² Spesso questi lavori sono attinenti ad un settore politico come ad esempio la politica energetica, la politica dei trasporti o la politica di sicurezza. I lavori si limitano però spesso a singoli settori, singoli pericoli o contromisure specifiche. In genere, inoltre, l'approccio metodologico varia da un progetto all'altro, ad esempio per la valutazione dei pericoli o per la deduzione di contromisure.
- Nei settori politici specifici delle infrastrutture critiche, agli aspetti relativi alla protezione viene però spesso attribuita un'importanza secondaria e la tematica non viene affrontata in modo sufficientemente esplicito e particolareggiato. Tuttavia l'importanza delle infrastrutture critiche aumenta costantemente, a causa ad esempio della sempre maggiore tecnologizzazione, e la Svizzera dipende sempre più da un'infrastruttura sempre funzionante. Oggi un'interruzione importante dell'approvvigionamento di energia elettrica o delle telecomunicazioni avrebbe conseguenze molto più gravi di quante ne avrebbe avuta alcuni anni fa. Anche i pericoli che causano interruzioni di questo tipo (minaccia cibernetica, terrorismo, aumento delle catastrofi naturali ecc.) sono cambiati, come è aumentata la vulnerabilità delle infrastrutture critiche, non da ultimo poiché oggi sono spesso costituite da sistemi transfrontalieri, in cui anche perturbazioni di piccola entità possono avere ripercussioni a livello internazionale. Senza dimenticare che in molti luoghi i processi di produzione e di distribuzione sono stati automatizzati e le ridondanze eliminate.
- Nel giugno del 2009 il Consiglio federale ha approvato la strategia di base per la protezione delle infrastrutture critiche.³ Questa ha permesso di migliorare il coordinamento e le basi in campo PIC; il modo di procedere sistematico e globale non è però ancora applicato in tutti i settori.

² Nel sottosettore «Approvvigionamento energetico», ad esempio, la Confederazione ha elaborato tra l'altro una strategia «reti energetiche» con l'obiettivo di garantire una rete elettrica sicura e sempre performante. Un programma della Confederazione per la mitigazione dei terremoti si occupa inoltre di incrementare la resistenza sismica dell'infrastruttura elettrica. Per ridurre l'entità dei danni in caso d'evento, l'Approvvigionamento economico del Paese elabora piani per la gestione dell'elettricità in caso di crisi, applicati dall'Organizzazione per l'approvvigionamento di corrente elettrica in situazioni straordinarie (OACCESS).

³ La strategia di base PIC è disponibile sul sito: www.protpop.admin.ch > Temi > Protezione delle infrastrutture critiche

4.2 Strategie PIC all'estero

Negli ultimi anni diversi Stati hanno adottato o aggiornato strategie nazionali in materia di protezione delle infrastrutture critiche. Un confronto mostra che gli aspetti principali presi in considerazione sono i seguenti.

- Incentivazione del dialogo e della collaborazione (all'interno e tra settori specifici) grazie alla creazione di piattaforme (Germania) o «secretariats» (USA, Australia) in cui sono rappresentati le autorità e i gestori delle infrastrutture critiche.
- Elaborazione di un elenco di infrastrutture critiche, rispettivamente identificazione di singoli oggetti (tra l'altro Francia e Germania). Le infrastrutture critiche vengono in parte definite solo in modo generico (p. es. «centrali energetiche»), senza specificare di che tipo di oggetto si tratta esattamente. Anche l'Unione europea sta stilando un elenco delle infrastrutture critiche nei settori energia e trasporti a livello europeo, focalizzato sugli effetti transfrontalieri di interruzioni di infrastrutture critiche.
- Elaborazione di piani e concetti di protezione per le infrastrutture identificate come critiche; in genere al termine di un processo quadro indicato nella strategia (in particolare USA).

Il confronto mostra inoltre che nessuna delle strategie prese in esame fornisce indicazioni in merito a deficit in singoli settori delle infrastrutture critiche, a singole contromisure o ai costi generati da eventuali provvedimenti. Esse mirano invece sempre a garantire un procedimento globale e unitario.

5 Situazione auspicata e obiettivo della strategia nazionale PIC

5.1 Situazione auspicata

La situazione auspicata con la strategia nazionale PIC è la 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 connessi e limitare l'entità dei danni in caso d'evento».

5.2 Obiettivo

L'obiettivo della strategia nazionale per la protezione delle infrastrutture critiche è rafforzare la resilienza della Svizzera in relazione alle infrastrutture critiche e garantire il coordinamento di tutti gli organi coinvolti.

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 (infrastrutture critiche, Stato, economia e società) di per sé;
2. la disponibilità di ridondanze;

3. la capacità di mobilitare misure di sostegno efficaci;
4. la tempestività e l'efficienza delle misure di sostegno.

In base a queste considerazioni, gli obiettivi della strategia nazionale PIC vengono suddivisi in due settori. La strategia nazionale PIC deve pertanto:

- rafforzare la robustezza e la flessibilità delle infrastrutture critiche;
- a livello intersettoriale, migliorare la collaborazione, la robustezza e la flessibilità della società, dell'economia e dello Stato (Confederazione, Cantoni e Comuni) e garantire che in vista di un sinistro siano disponibili rapidamente misure di sostegno e ridondanze efficaci.

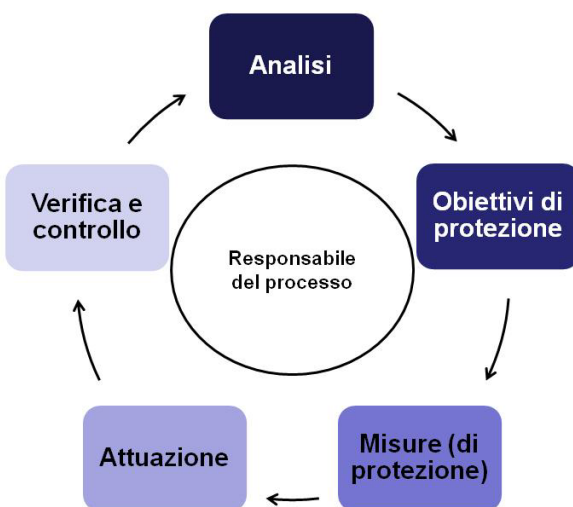
Per raggiungere questi obiettivi ci si propone di migliorare la *protezione integrale* (cfr. n. 6) con l'ausilio di un procedimento armonizzato e coordinato.

6 Protezione integrale

La protezione integrale si basa su un processo sistematico diretto dall'organo competente di caso in caso (questi organi sono definiti al n. 8).

Figura 1

Processo di protezione integrale



Gli obiettivi da raggiungere sono i seguenti:

Analisi

- Identificare e prioritizzare i processi critici, i sistemi, gli oggetti ecc.
- Identificare e valutare i rischi e i punti vulnerabili che potrebbero portare a interruzioni importanti

- Individuare per tempo i cambiamenti rilevanti nell'ambito delle minacce per le infrastrutture critiche

Obiettivi di protezione

- Gli obiettivi di protezione e di prestazione sono fissati a livello politico e applicati a livello aziendale.

Misure (di protezione):

- In base agli obiettivi di protezione e di prestazione concordati, i rispettivi organi definiscono le misure (compresi concetti, strutture, processi e strumenti) che consentono di
 - evitare nel limite del possibile interruzioni gravi su vasta scala,
 - proteggere dalle minacce e far fronte agli eventi e
 - tornare rapidamente al funzionamento normale.

Le misure si basano su un approccio costo-efficacia basato sul rischio.

Attuazione

- Le misure definite sono applicate.

Verifica e controllo

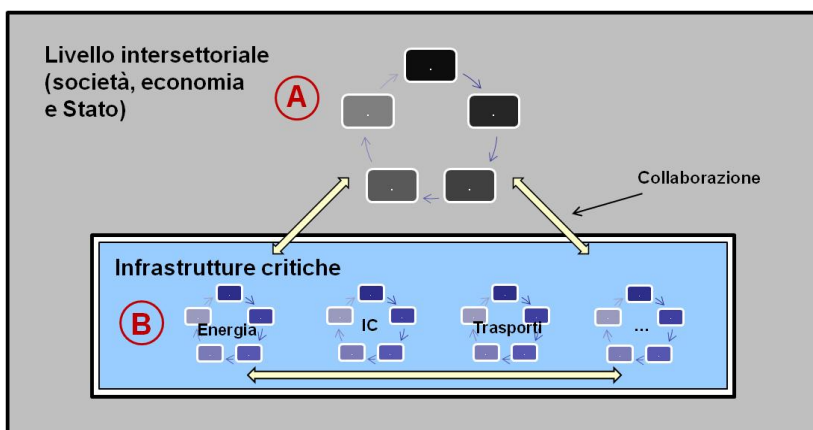
- L'effetto delle misure adottate è verificato.
- Le misure sono addestrate nell'ambito di esercitazioni.

7 Misure nell'ambito della strategia nazionale PIC

Conformemente agli obiettivi (cfr. n. 5), la strategia nazionale PIC elenca le misure volte a rafforzare la *protezione integrale* in due settori (campi d'azione):

- a *livello intersettoriale*, per garantire il coordinamento e migliorare la robustezza della società, dell'economia e dello Stato in vista di interruzioni delle infrastrutture critiche (*campo d'azione A*). A questo scopo vengono elaborati processi validi per diverse infrastrutture critiche (p. es. per migliorare il coordinamento e per sostenere i gestori in caso d'evento) e adottate misure atte a ridurre la vulnerabilità della società, dell'economia e dello Stato nei confronti di interruzioni delle infrastrutture critiche;
- a *livello delle infrastrutture critiche*, per rafforzare l'autoprotezione risp. la robustezza delle singole infrastrutture critiche (*campo d'azione B*). A questo scopo vengono identificati e ridotti i rischi specifici. Migliorando l'autoprotezione delle singole infrastrutture e garantendo un procedimento unitario e la compatibilità delle misure, si riducono automaticamente anche i rischi legati alle interdipendenze.

Campi d'azione della strategia nazionale PIC



Di seguito sono elencate le misure per questi due campi d'azione volte a raggiungere gli obiettivi descritti nei numeri precedenti della presente strategia.

Come illustrato nel numero 4.1, in relazione alla protezione delle infrastrutture critiche sono già in corso o previsti diversi progetti, piani e misure importanti. Nell'ambito dell'attuazione della strategia nazionale PIC si tratterà quindi spesso di verificare processi già esistenti ed eventualmente di completarli. Dove possibile, la strategia nazionale PIC si fonda su elementi già esistenti. Il confronto dettagliato è assicurato nell'ambito della pianificazione dell'attuazione. L'allegato alla strategia offre un quadro generale dei provvedimenti e delle correlazioni con altri lavori in materia; nel testo si rinuncia volutamente ad una citazione esplicita.

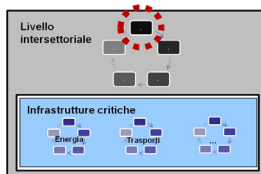
7.1 Rafforzare la protezione integrale a livello intersettoriale (campo d'azione A)

La protezione integrale a livello intersettoriale comprende tutte le attività necessarie per l'elaborazione, la gestione e lo sviluppo delle attività importanti per la protezione delle infrastrutture critiche. L'obiettivo è aumentare la resilienza dello Stato, dell'economia e della società e creare le condizioni quadro necessarie per la protezione delle infrastrutture critiche. I provvedimenti si basano sulla protezione integrale descritta nel numero 6, mentre le fasi di attuazione nonché di verifica e controllo sono trattate nel numero 8 della presente strategia.

Analisi

Identificare e prioritizzare le infrastrutture critiche

Prima di adottare delle misure di protezione, gli organi competenti devono sapere quali infrastrutture sono particolarmente critiche. Conoscenze sulle infrastrutture critiche e la loro importanza sono necessarie anche per effettuare valutazioni della situazione in caso d'evento.



In base alla strategia PIC del Consiglio federale viene pertanto elaborato l'inventario delle infrastrutture critiche (Inventario PIC). Esso riporta sia i singoli oggetti (costruzioni e impianti) critici a livello nazionale, sia quelli critici a livello cantonale e locale. Nel limite del possibile si ricorre a dati già rilevati nell'ambito di altri elenchi.

Obiettivo:

- Le infrastrutture critiche del Paese sono identificate e censite, corredate di dati attuali, nel rispetto delle prescrizioni sulla protezione delle informazioni (nel caso di informazioni classificate). Sono individuati e prioritizzati soprattutto i sistemi e gli oggetti critici.

Misura:

- *M1*: Tenere un elenco periodicamente aggiornato delle infrastrutture critiche del Paese (Inventario PIC) che permetta di elaborare tempestivamente estratti per diversi utenti nel rispetto della protezione delle informazioni. In quest'ottica occorre verificare la possibilità di attingere a elenchi già esistenti nel rispetto delle basi legali.

Conoscere i rischi, la vulnerabilità e le possibilità di protezione

Per migliorare la protezione integrale delle infrastrutture critiche sono necessarie informazioni intersettoriali sui rischi rilevanti. Molto utile a questo scopo è un catalogo dei possibili rischi con indicazioni sull'occorrenza e l'entità dei danni. A livello delle singole infrastrutture questi scenari sono completati con osservazioni concrete.

Per lo sviluppo metodologico sono inoltre necessari dati scientifici fondati, ad esempio nei settori delle interdipendenze e delle analisi di criticità. È inoltre necessario seguire lo sviluppo di nuove tecnologie e altri tipi di sviluppi (ambiente, contesto generale) che potrebbero comportare nuovi rischi.

Obiettivi:

- Elaborare un compendio periodicamente aggiornato dei pericoli rilevanti con una valutazione della loro occorrenza e dell'entità dei danni.
- Elaborare basi scientifiche fondate che consentano uno sviluppo metodologico della protezione integrale.

Misura:

- *M2*: Lanciare dei programmi di ricerca (p. es. programma di ricerca nazionale) finalizzati all'ottenimento di basi metodologiche su temi intersettoriali come l'analisi delle interdipendenze e della criticità, la misurazione della resilienza o gli sviluppi tecnologici.

Migliorare la collaborazione e lo scambio di informazioni

Le infrastrutture critiche presentano un elevato grado d'interdipendenza. La collaborazione e il dialogo sui rischi e le possibili misure di protezione (*best practice*) tra le diverse infrastrutture critiche è quindi di primaria importanza. La collaborazione deve essere migliorata sia tra i gestori delle infrastrutture, sia tra le autorità e gli organi specializzati competenti. Dato che le infrastrutture critiche costituiscono spesso sistemi transfrontalieri, occorre dare la necessaria importanza anche alla collaborazione internazionale.

Obiettivo:

- Istituire uno scambio d'informazioni intersettoriale e istituzionalizzato sui rischi, la vulnerabilità e le possibili misure di protezione (*best practice*) nel rispetto della protezione delle informazioni (nel caso di informazioni classificate).

Misura:

- *M3*: Creare piattaforme per incentivare la collaborazione tra organi specializzati e autorità attive nei diversi settori della protezione delle infrastrutture critiche (gruppo di lavoro PIC), tra i gestori delle infrastrutture critiche (gruppo di lavoro gestori) e con i partner esteri nell'ambito della protezione delle infrastrutture critiche.

Assicurare l'allerta in caso d'evento

In caso di minaccia acuta un'allerta tempestiva è cruciale al fine dell'adozione tempestiva di contromisure adeguate. A tal fine è necessario riconoscere i cambiamenti (repentini) della situazione di minaccia. Per diversi pericoli esistono procedure invalse atte a riconoscere per tempo questi cambiamenti. Ciò non è però garantito in egual misura per tutti i pericoli rilevanti (in particolare non per quelli tecnologici). Bisogna inoltre garantire che l'allerta avvenga in tempo utile e attraverso interfacce ben definite. Anche qui esistono già diversi meccanismi invalsi. Tuttavia una buona parte non dispone di sufficienti risorse (in personale), oppure non sono integrati tutti i gestori conformemente alla loro importanza. Determinati processi non sono inoltre canalizzati e fanno riferimento a persone di contatto differenti.

Obiettivi:

- I cambiamenti (repentini) rilevanti della situazione di minaccia nell'ambito di uno spettro di pericoli integrale sono riconosciuti in tempo utile.
- In caso di minaccia acuta i gestori di infrastrutture critiche vengono avvisati per tempo e anche in situazioni straordinarie con uno standard qualitativo conforme alla loro importanza. Si assicura che lo spettro di pericoli coperto sia completo, che il processo d'allerta avvenga con l'ausilio di collegamenti sicuri o protetti tramite contatti ben definiti e che la protezione delle informazioni sia garantita.

Misure:

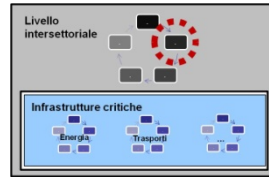
- *M4*: Le competenze e le capacità per il riconoscimento e la sorveglianza dei pericoli e delle minacce devono essere verificate nell'ottica di tutte le situazioni possibili.

- M5: In base ai processi e alle strutture esistenti deve essere messo in atto un meccanismo che garantisca che tutti i gestori rilevanti di infrastrutture critiche vengano informati per tempo in merito a cambiamenti significativi della situazione di minaccia.

Obiettivi di protezione

Definire obiettivi di protezione superiori

Gli obiettivi di protezione forniscono informazioni sul livello di prestazioni e di protezione auspicato. Essi sono fissati da politica e società. È auspicabile che per le diverse infrastrutture critiche vengano definiti obiettivi di protezione armonizzati e vincolanti nell'ambito di un processo politico. Considerata l'eterogeneità delle infrastrutture critiche e dell'importanza politica dell'argomento, ciò rappresenta un compito estremamente difficile. Per questo motivo la situazione auspicata descritta nella strategia funge da obiettivo di protezione a livello intersettoriale. Gli obiettivi di protezione vengono concretizzati nell'ambito delle singole infrastrutture critiche al momento dell'elaborazione dei piani di protezione integrale (cfr. misura M15). Se possibile, a questo scopo si ricorre alle revisioni delle basi legali esistenti, sempre tenendo conto degli obiettivi di protezione già esistenti.



Obiettivo:

- Per le diverse infrastrutture critiche sono definiti obiettivi di protezione concertati.

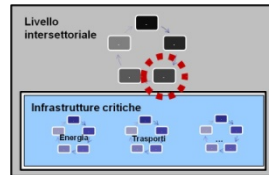
Misura:

- M6: Formulare obiettivi di protezione concertati tra loro e politicamente avallati.

Misure (di protezione)

Evitare interruzioni delle infrastrutture critiche

A livello intersettoriale è possibile adottare diversi provvedimenti per ridurre i rischi rilevanti per tutti i tipi di infrastrutture critiche ed evitare così interruzioni importanti. I rischi generici di questo tipo riguardano ad esempio il personale responsabile per lo svolgimento di processi chiave. Al fine di soddisfare standard di sicurezza elevati e permettere lo scambio di informazioni classificate, dovrebbe essere possibile sottoporre tali persone ad un controllo di sicurezza. Un altro rischio generico è costituito dall'approvvigionamento delle infrastrutture critiche con energie e mezzi di telecomunicazione. A questo proposito le infrastrutture critiche devono incrementare la loro autoprotezione nell'ambito del campo d'azione B (cfr. n. 7.2). Inoltre, le infrastrutture critiche a livello nazionale devono essere trattate, nel limite delle possibilità tecniche, in modo prioritario nell'ambito dei progetti di prioritizzazione e dei piani aziendali.



Obiettivi:

- Le persone che hanno accesso a processi chiave⁴ nel campo delle infrastrutture critiche sono sottoposte a un controllo di sicurezza.
- In caso di misure di gestione o di interruzioni nel settore energetico e delle telecomunicazioni, nel limite delle possibilità tecniche le infrastrutture critiche a livello nazionale vengono trattate in modo prioritario.

Misure:

- *M7:* Creare una base legale che permetta di sottoporre determinate categorie di personale dei gestori di infrastrutture critiche a controlli di sicurezza.
- *M8:* Completare, nel limite delle possibilità tecniche, i piani d'interruzione e/o di gestione esistenti con le infrastrutture critiche nazionali.

Migliorare la preparazione dello Stato, dell'economia e della popolazione

Interruzioni importanti di infrastrutture critiche possono compromettere seriamente il funzionamento dello Stato e dell'economia e comportare gravi disagi per la popolazione. L'entità dei danni può essere ridotta se lo Stato, l'economia e la popolazione sono adeguatamente preparati. Per questo motivo viene attribuita grande importanza alle pianificazioni preventive per la gestione degli eventi e alla sensibilizzazione preliminare della popolazione e dell'economia sui possibili rischi e sulle misure preventive personali.

Obiettivo:

- Lo Stato, l'economia e la popolazione sono preparati in vista di gravi interruzioni di infrastrutture critiche, in modo tale da permettere di ridurre gli effetti e di gestire l'evento.

Misure:

- *M9:* Confederazione e Cantoni elaborano pianificazioni preventive per la gestione di interruzioni gravi di infrastrutture critiche.
- *M10:* La popolazione e l'economia vengono informate e sensibilizzate in merito alle possibilità di prevenzione personali in caso di interruzione di infrastrutture critiche.

Sostenere i gestori di infrastrutture critiche nella gestione degli eventi

In caso di minaccia acuta o di interruzioni gravi, i gestori dovrebbero essere sussidiariamente sostenuti con mezzi o capacità extra-aziendali al fine di combattere la minaccia o di rendere possibile un funzionamento minimo e il rapido ritorno al funzionamento normale.⁵ Affinché ciò sia possibile, in primo luogo sono necessari i mezzi o le capacità corrispondenti. Mentre è già ora possibile ricorrere a forze d'intervento per far fronte alle minacce fisiche, non sono ancora disponibili mezzi pubblici sufficienti per combattere i rischi cibernetici di ampia portata (in particolare mancano le risorse in personale). Secondariamente è opportuno rilevare i mezzi e le rispettive necessità per il caso di situazioni straordinarie (in particolare per quanto

⁴ Questi processi saranno definiti nell'ambito dell'elaborazione dell'inventario PIC.

⁵ Si tratta ad esempio di forze d'intervento (polizia, pompieri, protezione civile, esercito), mezzi di comunicazione o gruppi elettrogeni d'emergenza.

concerne i gruppi elettrogeni d'emergenza e i mezzi di comunicazione). In terzo luogo si deve assicurare che l'attribuzione dei mezzi a livello strategico venga decisa tenendo conto della situazione di minaccia, dell'importanza (criticità) delle infrastrutture critiche e dei mezzi disponibili. In quarto luogo è opportuno elaborare pianificazioni preventive per garantire l'impiego efficace dei mezzi.

Obiettivo:

- I gestori delle infrastrutture critiche vengono sostenuti, tenendo conto della loro importanza, in modo sussidiario ed efficace con mezzi esterni al fine di combattere le minacce, garantire un funzionamento minimo e un rapido ritorno alla normalità.

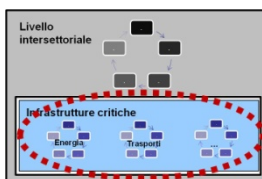
Misure:

- *M11:* Creare mezzi ufficiali sufficienti per il sostegno sussidiario dei gestori delle infrastrutture critiche nella lotta contro le minacce cibernetiche di grande entità.
- *M12:* Rilevare, in vista di situazioni straordinarie, le risorse disponibili per garantire un funzionamento minimo e il ritorno alla normalità.
- *M13:* Definire, d'intesa con gli organi interessati, i processi relativi all'attribuzione di mezzi esterni per sostenere i gestori nella gestione degli eventi.
- *M14:* Rafforzare la collaborazione tra gli organi di crisi e di condotta a livello federale, cantonale e comunale e i gestori delle infrastrutture critiche e allestire piani d'intervento per la protezione fisica delle infrastrutture critiche nazionali.

7.2 Migliorare la protezione integrale a livello delle singole infrastrutture critiche (campo d'azione B)

Oltre al livello intersettoriale la strategia nazionale PIC mira a rafforzare anche la protezione integrale nel campo delle singole infrastrutture critiche.

Dato che interruzioni gravi possono essere causate anche da rischi specifici riguardanti un singolo elemento critico (p. es. un posto di comando), un sotto-settore critico (p. es. rete di trasporti obsoleta) o un settore critico (p. es. trasporti), come definito al numero 6 la protezione integrale deve essere rafforzata a tutti i livelli delle infrastrutture critiche. A questo scopo devono essere elaborati e attuati piani di protezione integrale per le infrastrutture critiche. Il relativo procedimento deve essere



descritto ad esempio nell'ambito di linee guida elaborate sulla base della strategia PIC del Consiglio federale. Nei piani di protezione integrale sono rilevati e integrati i lavori in corso o pianificati, come pure le basi legali, gli obiettivi di protezione ecc. In seguito saranno individuati i rischi residui specifici delle singole infrastrutture, fissati gli obiettivi di protezione ed eventualmente elaborate le misure volte alla riduzione dei rischi. Si tratterà inoltre di analizzare come finanziare le eventuali misure di protezione necessarie e quali basi legali sono necessarie per attuare i piani di protezione integrale.

I piani di protezione integrale dovranno essere elaborati e attuati in collaborazione con i rispettivi organi competenti (autorità a livello federale, cantonale o comunale, gestori, servizi specializzati nei rischi o nelle misure, associazioni ecc.). La responsabilità (in particolare per quanto attiene alla determinazione degli obiettivi di protezione) è degli organi competenti secondo le vigenti basi legali. Di conseguenza, gli obiettivi di protezione e il finanziamento di eventuali misure successive sono convenuti nell'ambito dei settori politici specifici dei sottosectori. I lavori in tal senso si basano su un approccio costo-efficacia basato sul rischio, vale a dire che vengono adottate solo misure necessarie per raggiungere gli obiettivi di protezione, dove il rapporto costo-utilità deve risultare positivo. I piani di protezione integrale devono pertanto servire soprattutto ad ottenere un quadro completo dei rischi e delle vulnerabilità rilevanti, a verificare il livello di protezione esistente e a identificare e colmare eventuali lacune.

Obiettivo:

- La protezione integrale delle infrastrutture critiche è garantita a tutti i livelli interessati (settori critici, sottosectori critici e singoli elementi critici). Tutti i potenziali rischi sono individuati e ridotti secondo un approccio costo-efficacia basato sui rischi in base a obiettivi di prestazione e protezione concordati a livello politico. Lo spettro dei pericoli e delle misure preso in considerazione è il più ampio possibile.

Misura:

- *M15:* Elaborare, per esempio in base alla guida PIC, dei piani di protezione integrali per le infrastrutture critiche e attuarli in conformità a basi legali appropriate. I piani di protezione integrale devono essere elaborati e attuati in collaborazione con i rispettivi organi competenti (autorità direttive e specializzate a livello federale, cantonale e comunale, gestori, associazioni ecc.). Gli organi elencati nella tabella 2 determinano quali enti hanno funzioni direttive e quali devono essere coinvolti.

8 Attuazione della strategia nazionale PIC

8.1 Strutture e competenze

L'applicazione della strategia nazionale PIC si inserisce principalmente nel quadro dei processi collaudati e delle strutture e delle competenze esistenti. Il coordinamento è assicurato grazie al coinvolgimento precoce delle autorità competenti (a livello federale e cantonale), dell'economia (in particolare dei gestori delle infrastrutture critiche) e del mondo scientifico. In questo contesto è assicurata anche la collaborazione con il meccanismo di consultazione e di coordinamento Rete integrata Svizzera per la sicurezza (MCC RSS).

La segreteria PIC sostiene gli organi competenti nell'attuazione delle diverse misure ed è responsabile in particolare dei compiti seguenti:

- coordinare le misure conformemente al processo di protezione integrale a livello intersettoriale (tenuta dell'inventario PIC ecc.);
- sostenere le autorità competenti e i gestori nell'elaborazione di piani di protezione integrali nel campo delle infrastrutture critiche;

- fornire consulenza ai Cantoni nell'ambito di lavori rilevanti per la protezione delle infrastrutture critiche;
- preparare gli affari per le piattaforme di coordinamento;
- fungere da organo di contatto per le questioni PIC a livello internazionale;
- riferire sullo stato dell'attuazione della strategia nazionale PIC.

Un altro compito centrale è costituito dal coordinamento con lavori analoghi (tra l'altro strategia nazionale di difesa cibernetica, strategia sul futuro delle reti infrastrutturali, gestione dei rischi della Confederazione, approvvigionamento economico del Paese). Questo è assicurato attraverso uno scambio reciproco di risultati e uniformando i procedimenti metodologici a livello intersettoriale d'un canto e tenendo conto dei risultati dei lavori nell'ambito dei piani di protezione integrale a livello delle singole infrastrutture critiche (livello infrasettoriale) dall'altro.

La competenza per l'attuazione delle misure a livello intersettoriale (M1–M14) spetta agli organi indicati nell'allegato. Nell'ambito della sua responsabilità relativa ai processi, la segreteria PIC assume una funzione di coordinamento a livello intersettoriale. In collaborazione con gli organi citati verifica quali progetti, processi ecc. siano rilevanti nel contesto della rispettiva misura, in che misura gli obiettivi formulati nella strategia siano già raggiunti e quali provvedimenti siano ancora necessari. Nel limite del possibile le misure sono applicate nell'ambito dei progetti o delle attività in corso.

Un procedimento analogo è applicato anche nel campo delle singole infrastrutture critiche, dove la responsabilità per i processi di protezione integrale (M15) è di regola delle autorità competenti secondo le basi legali vigenti (Confederazione, Cantoni o Comuni). Gli organi elencati nella tabella 2 sono invitati a determinare, se del caso in collaborazione con la segreteria PIC, quali organi dirigono e quali devono essere coinvolti nell'elaborazione dei piani di protezione integrale. L'elaborazione ha luogo in collaborazione con i rispettivi organi competenti (gestori, associazioni, servizi specializzati su minacce e misure ecc.). Se necessario e nel limite delle possibilità la segreteria PIC può accompagnare i lavori.

Competenze specifiche dei sottosettori

Settore	Sottosettore (SST)	Organo federale coordinante (<i>elenco non esaustivo</i>)*
Autorità	Rappresentanze diplomatiche e sedi di organizzazioni internazionali	DFAE, fedpol
	Ricerca e insegnamento	SER
	Beni culturali	UFPP, UFC
	Parlamento, governo, giustizia, amministrazione	CaF, Servizi del Parlamento, fedpol, UFCL, ODIC e FP
Energia	Approvvigionamento di gas naturale	UFE, UFAE, IFO
	Approvvigionamento di petrolio	UFE, UFAE, IFO
	Approvvigionamento di energia elettrica	UFE, UFAE, EICOM, IFSN, ESTI
Smaltimento	Rifiuti	UFAM
	Acque di scarico	UFAM
Finanze	Banche	FINMA, BNS, AFF, SFI
	Assicurazioni	FINMA, UFAS
Sanità pubblica	Cure mediche e ospedaliere	SSC
	Laboratori	UFSP
Industria	Industrie chimiche e farmaceutiche	UFAE
	Industrie elettro-meccaniche e metallurgiche	UFAE
Informazione e comunicazione	Tecnologie dell'informazione	UFAE, ODIC
	Media	UFCEM
	Traffico postale	SG DATEC, UFCEM
	Telecomunicazioni	UFCEM, UFAE
Alimentazione	Approvvigionamento alimentare	UFAE, UFAG
	Approvvigionamento idrico	UFAM, UFAE
Sicurezza pubblica	Esercito	PIO
	Organizzazioni di primo intervento	UFPP, fedpol, SIC
	Protezione civile	UFPP
Trasporti	Traffico aereo	UFAC, UFAE
	Traffico ferroviario	UFT, UFAE
	Traffico navale	UFT, UFAE
	Traffico stradale	USTRA, UFAE

* Gli organi citati assumono un ruolo di coordinamento: in caso di necessità determinano, d'intesa con la segreteria PIC, quali organi dirigono (Confederazione, Cantoni, associazioni ecc.) e quali devono essere coinvolti nell'elaborazione dei piani di protezione integrale. Sono fatte salve le competenze esistenti.

8.2 Tempistica e controlling

Le singole misure sono realizzate con l'ausilio di un piano d'attuazione e di controlling dettagliato, che sarà elaborato una volta approvata la strategia nazionale PIC. A grandi linee l'attuazione deve avvenire con la tempistica seguente.

Fase 1 (entro la fine del 2012)

- Elaborazione dei piani d'attuazione.
- Identificazione e rilevamento delle infrastrutture critiche a livello nazionale. (M1)
- Creazione delle piattaforme intersettoriali (GL PIC e GL gestori). (M3)

Fase 2 (entro la fine del 2013)

- Preparare il concetto volto a garantire l'allerta in caso d'evento. (M5)
- Preparare le basi e le proposte per obiettivi di protezione concertati. (M6)
- Elaborare una proposta di legge per i controlli di sicurezza dei gestori di infrastrutture critiche. (M7)
- Completare i piani d'interruzione e di gestione esistenti con le infrastrutture critiche a livello nazionale. (M8)
- Sviluppare un meccanismo per il rilevamento delle risorse esistenti. Definire i processi per sostenere i gestori con mezzi esterni. (M12, M13)

Fase 3 (entro la fine del 2014)

- Presentare una proposta aggiornata per un programma di ricerca nazionale. Ulteriori accertamenti nel campo della ricerca settoriale sono conclusi. (M2)
- Ottenere i risultati necessari per la verifica delle competenze e delle capacità nell'ambito della sorveglianza delle minacce. (M4)
- Elaborare prodotti informativi incentrati sul rafforzamento dell'autoprevenzione da parte dell'economia e della popolazione. (M10)
- Elaborare pianificazioni d'intervento per la protezione fisica delle infrastrutture critiche. (M14)

Fase 4 (dal 2015)

- Elaborare pianificazioni preventive per la gestione di interruzioni di infrastrutture critiche. (M9)
- Creare, gradualmente, le risorse personali e le capacità per il sostegno sussidiario dei gestori nel fronteggiare i rischi cibernetici in base a relative basi legali. (M11)
- Elaborare e attuare piani di protezione integrale per le infrastrutture critiche. (M15)

Ogni quattro anni al Consiglio federale è presentato un rapporto sullo stato dell'attuazione.

8.3

Revisione della strategia PIC

La strategia nazionale per la protezione delle infrastrutture critiche è periodicamente aggiornata. La presente strategia è sottoposta a verifica ed eventualmente adattata entro la fine del 2016.

Misure e punti d'intersezione con lavori in corso o pianificati

Misure	Organi competenti (<i>elenco non esaustivo</i>)*	Punti d'intersezione con altri progetti/enti/organizzazioni (<i>elenco non esaustivo</i>)*
<i>M1</i> : Stesura dell'Inventario PIC	UFPP, organi federali secondo la tabella 2, Cantoni (interlocutori cantonali in materia PIC)	Elenchi e inventari esistenti (catasto delle perturbazioni, impianti d'accumulazione, beni culturali ecc.)
<i>M2</i> : Lancio di programmi di ricerca (compreso programma di ricerca nazionale)	UFPP	Fondo nazionale svizzero (FNS), programmi di ricerca degli enti federali
<i>M3</i> : Creazione di piattaforme autorità/ servizi specializzati e gestori	UFPP	Approvvigionamento economico del Paese (AEP), Servizio delle attività informative della Confederazione (SIC), Strategia nazionale di difesa cibernetica
<i>M4</i> : Verifica delle competenze e delle capacità per la sorveglianza dei pericoli	UFAM, UFAE, MeteoSvizzera, SIC	Piattaforma informativa comune sui pericoli naturali, Elaborazione legge sul servizio delle attività informative, Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, AEP, strategia di difesa cibernetica
<i>M5</i> : Realizzazione di un meccanismo di allerta precoce	UFPP, UFAM, UFAE, MeteoSvizzera, SIC	Progetto Netaalert (UFPP), Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), AEP
<i>M6</i> : Elaborazione di obiettivi di protezione superiori	UFPP	Piattaforma interdepartimentale Pericoli naturali PLANAT, AEP

Misure	Organi competenti (<i>elenco non esaustivo</i>)*	Punti d'intersezione con altri progetti/enti/organizzazioni (<i>elenco non esaustivo</i>)*
<i>M7</i> : Creazione di una base legale per i controlli di sicurezza dei gestori di infrastrutture critiche	PIO	Progetto per una base legale formale per la protezione delle informazioni (FOGIS), Protezione delle informazioni e delle opere (PIO)
<i>M8</i> : Adattamento dei piani d'interruzione e di gestione esistenti	UFAE	UFE, ELCOM
<i>M9</i> : Elaborazione di pianificazioni preventive in previsione di interruzioni IC	UFPP, Cantoni (organi cantonali di condotta OCantC), UFAE, UFE	Stato maggiore federale NBCN (SMF NBCN), analisi cantonali dei rischi (KATAPLAN), AEP, IDA Nomex
<i>M10</i> : Miglioramento della preparazione dell'economia e della popolazione	UFPP, UFAE, CaF	Progetto misure di protezione individuali (UFPP), CaF
<i>M11</i> : Determinazione di aiuti sussidiari per la gestione delle minacce cibernetiche	SIC, OSIC, UFAE	Strategia nazionale per la protezione dai rischi cibernetiche
<i>M12</i> : Rilevamento di risorse per il funzionamento d'emergenza delle infrastrutture critiche	UFPP	Gestione delle risorse della Confederazione (ResMaB), AEP
<i>M13</i> : Determinazione di processi per l'attribuzione di mezzi esterni ai gestori di infrastrutture critiche	UFPP	Rete integrata Svizzera per la sicurezza (RSS), SMF NBCN, ResMaB, AEP, IDA Nomex
<i>M14</i> : Rafforzamento della collaborazione tra organi di condotta e gestori di infrastrutture critiche ed elaborazione di piani di protezione	SMF NBCN, Cantoni, Comuni (organi di condotta, polizia, pompieri), SMCOEs	RSS, sviluppo ulteriore protezione della popolazione/protezione civile, KATAPLAN, IDA NOMEX

Misure	Organi competenti (<i>elenco non esaustivo</i>)*	Punti d'intersezione con altri progetti/enti/organizzazioni (<i>elenco non esaustivo</i>)*
<i>M15</i> : Elaborazione e attuazione di piani di protezione integrali per le infrastrutture critiche	D'intesa con gli organi di coordinamento elencati nella tabella 2	Diversi lavori specifici dei settori e dei rischi (tra l'altro strategia per una società dell'informazione in Svizzera, strategia di difesa cibernetica, mitigazione del rischio sismico, gestione dei rischi della Confederazione, prioritizzazione di edifici federali in caso di interruzione di corrente)
* La segreteria PIC assume una funzione di coordinamento e assicura, in collaborazione con gli organi citati, il coinvolgimento di tutti gli organi competenti e rilevanti.		