Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Organo direzione informatica della Confederazione ODIC

Strategia nazionale per la protezione della Svizzera contro i cyber-rischi

Piano di attuazione SNPC

15 maggio 2013

Indice

1 Situazione iniziale

Adottando il 27 giugno 2012 la «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi» (SNPC) il Consiglio federale ha posato la prima pietra di una trattazione integrale della problematica cyber. La SNPC è incentrata al riguardo sull'avvertimento precoce dei cyber-rischi e delle minacce incombenti, su un rafforzamento generale della resistenza (resilienza) delle infrastrutture svizzere e su una riduzione generale dei cyber-rischi. La strategia comprende 16 misure concrete ripartite su 7 campi d'azione. Esse devono essere attuate e trasferite nell'esercizio regolare entro il 2017.

Campi d'azione e misure:

Campo d'azione 1	**Misure**	
ricerca e sviluppo	1	Ricerche in merito ai nuovi rischi in relazione con la problematica del cyberspazio.
Campo d'azione 2	**Misure**	
Analisi dei rischi e della vulnerabilità	2	Verifica autonoma dei sistemi. Analisi dei rischi per la minimizzazione dei rischi in collaborazione con le autorità, i fornitori di prestazioni TIC e i fornitori di sistemi.
	3	Verifica – a livello di sistemi, di organizzazione e di caratteristiche tecniche – della vulnerabilità dell'infrastruttura TIC.
Campo d'azione 3	**Misure**	
Analisi della situazione di minaccia	4	Elaborazione della rappresentazione e dell'evoluzione della situazione.
	5	Elaborazione di eventi per l'ulteriore sviluppo di misure.
	6	Panoramica dei casi e coordinamento dei casi di portata intercantonale.
Campo d'azione 4	**Misure**	
Creazione di competenze	7	Allestimento di una panoramica delle offerte di formazione in materia di creazione di competenze e individuazione delle lacune.
	8	Eliminazione delle lacune riscontrate nell'ambito delle offerte di formazione in materia di creazione di competenze e incremento dell'impiego di offerte di elevata qualità.
Campo d'azione 5	**Misure**	
Relazioni e iniziative internazionali	9	Partecipazione attiva della Svizzera nel settore dell'Internet governance.
	10	Cooperazione al livello della politica di sicurezza internazionale.
	11	Coordinamento degli attori in occasione della partecipazione a iniziative e «best practices» nell'ambito dei processi di sicurezza e di protezione.
Campo d'azione 6	**Misure**	
Gestione della continuità operativa e gestione delle crisi	12	Rafforzamento e miglioramento della resistenza (resilienza) nei confronti di perturbazioni e di eventi.
	13	Coordinamento delle attività in primo luogo con gli attori direttamente interessati e appoggio dei processi decisionali mediante competenze specialistiche.
	14	Misure attive per l'identificazione degli autori ed eventuale perturbazione della loro infrastruttura nel caso di una minaccia specifica.
	15	Elaborazione di un concetto per procedure e processi di condotta volti alla soluzione tempestiva dei problemi.
Campo d'azione 7	**Misure**	
Basi legali	16	Verifica delle basi legali vigenti in base alle misure e ai concetti d'attuazione e definizione delle priorità per quanto riguarda gli adeguamenti immediati.

L'ipotesi di base della strategia è che i cyber-rischi costituiscono l'espressione di rischi esistenti a livello di processi e di strutture. I cyber-rischi traggono origine dall'utilizzazione di sistemi TIC (in rete) sui quali sono viepiù eseguiti ed esercitati ogni genere di processi. Si può trattare dell'invio di un'informazione a mezzo e-mail, invece che per posta ordinaria, oppure della manipolazione di complessi impianti di comando e di produzione mediante un computer al posto di una manipolazione manuale. L'identificazione dei cyber-rischi deve pertanto fondarsi su una valutazione possibilmente esatta della situazione effettiva di minaccia e delle

sue interconnessioni. Le misure destinate a minimizzare i rischi non devono tuttavia concentrasi sulla sola sicurezza TIC. Le misure per ridurre al minimo i cyber-rischi debbono sempre prendere in considerazione e porre in sintonia tra di loro le dimensioni fisiche, personali, tecniche e organizzative che ne risultano. A livello nazionale questo può avvenire solo se ognuno assume le proprie responsabilità e se si coordinano le misure.

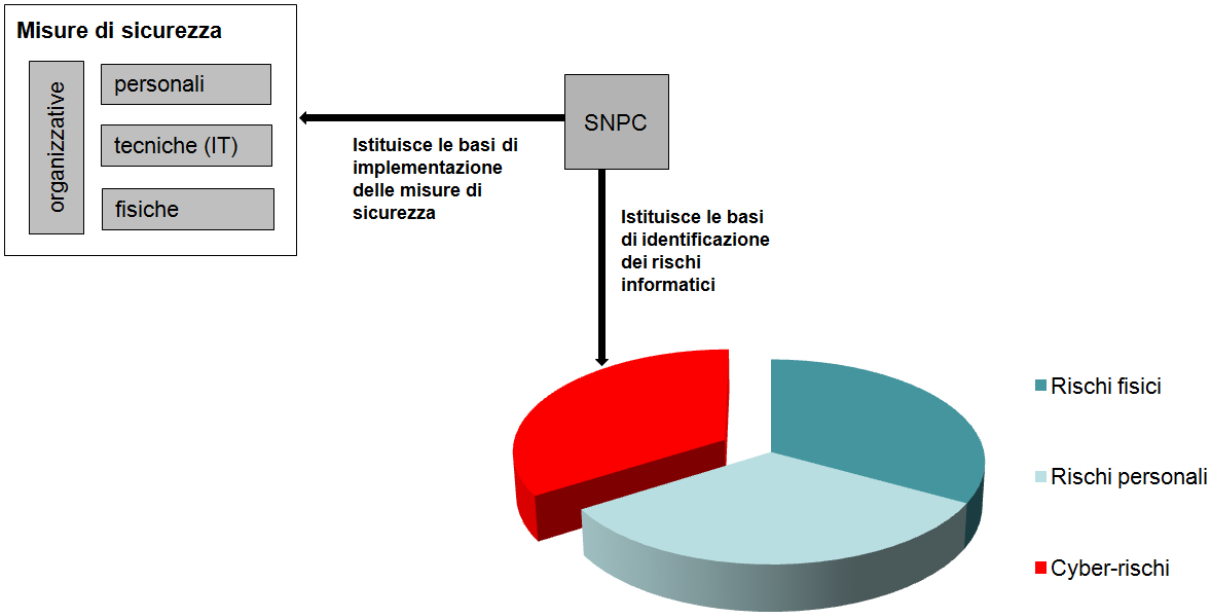

Figura 1: Cyber-rischi e misure di sicurezza

L'attuazione della strategia deve essere effettuata da un servizio di coordinamento integrato nel DFF e più precisamente nell'Organo direzione informatica della Confederazione (ODIC). Questo servizio di coordinamento (SC SNPC) deve elaborare un piano di attuazione della strategia unitamente ai propri partner a livello di Confederazione e di Cantoni e dal 2014 documentare al riguardo in maniera trasparente e completa l'eventuale maggiore fabbisogno di personale dei dipartimenti partecipanti e della Cancelleria federale.

Per quanto riguarda la protezione delle infrastrutture critiche (IC), la SNPC si fonda sulla «Strategia nazionale per la protezione delle infrastrutture critiche» (Strategia PIC) dell'Ufficio federale della protezione della popolazione (UFPP). Le analisi di rischio e di vulnerabilità previste nel quadro del programma PIC sono altresì destinate a identificare i cyber-rischi e a istituire quindi la base di una riduzione dei rischi uniforme e specifica ai settori. L'analisi dei rischi e delle vulnerabilità tiene conto dei settori e dei settori parziali definiti nella Strategia PIC. Partecipano a questo processo i regolatori e le autorità di vigilanza competenti, come pure l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) e l'UFPP. L'UFAE[1] e il UFPP[2] hanno la competenza dell'allestimento di un'analisi dei rischi e delle vulnerabilità per quanto riguarda i settori parziali loro attribuiti. Ove possibile e opportuno il modo di procedere e la metodologia dovranno essere stabiliti d'intesa tra l'UFAE e l'UFPP. Nella misura del possibile va pure seguito un approccio uniforme.

[1] I 13 settori parziali dell'UFAE sono: energia (approvvigionamento in gas naturale, in petrolio, in elettricità); industria (industria chimica e farmaceutica, industria metalmeccanica ed elettrica); informazione e comunicazione (tecnologie dell'informazione, telecomunicazione); alimentazione (approvvigionamento alimentare, approvvigionamento in acqua potabile); trasporti (trasporto aereo, trasporto su rotaia, navigazione, circolazione stradale).

[2] I 15 settori parziali dell'UFPP sono: autorità (Parlamento, giustizia, amministrazione; ricerca e insegnamento,beni culturali, organizzazioni internazionali); smaltimento (acque di scarico, smaltimento dei rifiuti); finanze (banche, assicurazioni); sanità (assistenza medica e ospedali, laboratori); informazione e comunicazione (media, traffico postale); pubblica sicurezza (esercito, organizzazioni di primo intervento, protezione civile).

Il consolidamento dei risultati sotto forma di analisi complessiva della situazione di minaccia è effettuato in collaborazione con la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

Le dipendenze e i punti di congiunzione possono essere riepilogati come segue:

- la strategia nazionale PIC si applica come strategia mantello al settore delle infrastrutture critiche della Svizzera e comprende la protezione delle infrastrutture critiche contro i cyber-rischi;
- le misure in ambito di SNPC che riguardano le infrastrutture critiche sono armonizzate con le misure della strategia PIC (p. es. analisi dei rischi e delle vulnerabilità);
- l'attuazione delle misure della strategia in ambito di infrastrutture critiche è effettuata in stretta collaborazione con l'UFAE, l'UFPP e l'ODIC.

Per concretizzare queste misure il SC SNPC ha in un primo tempo avviato colloqui con gli uffici federali coinvolti (cfr. capitolo 7), raccogliendo informazioni che ha successivamente consolidato. In questo ambito sono stati rilevati lo stato attuale e l'ulteriore pianificazione in vista dell'attuazione della strategia. Al riguardo sono emerse le seguenti informazioni:

a) l'approccio della responsabilità propria e la sussidiarietà della Confederazione, come perseguiti nella strategia, sono corretti;
b) ad avvenuta esecuzione delle analisi di rischio e di vulnerabilità previste possono subentrare, a motivo di interessi nazionali sovraordinati, una necessità di intervento e maggiori costi di soppressione dei rischi esistenti;
c) alcuni dipartimenti hanno già effettuato lavori preliminari per l'attuazione di misure nel quadro dei loro compiti;
d) occorre documentare un evidente fabbisogno di risorse.

Il presente piano di attuazione del DFF costituisce la base per dipartimenti e Uffici in vista della concretizzazione e dell'implementazione delle pertinenti misure. Il piano non si esprime concretamente sui compiti e sugli obblighi esatti dei servizi da istituire perché ciò compete ovviamente alla singola organizzazione, che si basa ad hoc sulle esperienze acquisite nell'ambito dell'attività quotidiana. Il punto di partenza sono le misure stabilite dalla strategia e da attuare e trasporre nell'esercizio regolare entro la fine del 2017.

I Cantoni sono integrati in questo processo di attuazione tramite il Meccanismo di consultazione e coordinamento nel quadro della Rete integrata Svizzera per la sicurezza (MCC RSS). Il SC SNPC deve inoltre sostenere in collaborazione con il MCC RSS un «gruppo specializzato cyber», in seno al quale sono rappresentati la Confederazione, i Cantoni e i Comuni.

La SNPC esclude esplicitamente il caso di guerra o di conflitto. L'esercito è personalmente responsabile in tutte le situazioni della protezione e della difesa delle proprie infrastrutture e dei propri sistemi. Entro il suo ambito di compiti e di responsabilità esso deve inoltre formulare approcci di soluzione anche per fare fronte alle cyber-minacce e alle loro ripercussioni. Il capo dell'esercito ha designato al riguardo un delegato alla cyber-difesa che ha iniziato la propria attività il 1° gennaio 2013.

2 Mandato e condizioni quadro

Dato che l'incremento della sicurezza perseguito nel contesto dei cyber-rischi può essere raggiunto unicamente attraverso la cooperazione di amministrazione, autorità cantonali, settori e settori parziali e gestori di infrastrutture critiche, questa strategia coinvolge tutti gli attori nell'attuazione delle misure.

Il piano di attuazione è stato allestito con il forte coinvolgimento dell'UFAE e dell'UFPP. Anche il MCC RSS, che costituisce l'interfaccia di Confederazione e Cantoni, è stato coinvolto come partner centrale per l'attuazione.

3 Informazioni acquisite

3.1 Fabbisogno di risorse

Le stime del fabbisogno sono state consolidate nel quadro di interviste e poggiano su documentazioni esistenti del fabbisogno e pareri scritti degli uffici rilevanti in questo ambito, oppure si desumono dalle misure della presente strategia. Vi è fabbisogno di risorse perché la percezione del cyber-aspetto dei processi già esistenti nell'Amministrazione federale per l'attuazione delle misure della SNPC va di pari passo con maggiori oneri.

Da parte di diversi uffici perviene la richiesta di conoscenze peritali approfondite su tematiche analoghe nel settore cyber. Per costituire in comune questo sapere e poi trasmetterlo sono state discusse apposite forme di collaborazione. In questo senso ad esempio per il settore di regolamentazione, dal quale risulteranno poi sinergie per le autorità specializzate come tra l'altro l'Ufficio federale dell'aviazione civile (UFAC), l'Ufficio federale delle strade (USTRA), l'Ufficio federale dell'energia (UFE). In questo ambito sussiste le necessità di dibattere in comune le problematiche dei cyber-rischi consecutivi all'impiego crescente di sistemi di pilotaggio e di controllo. Una collaborazione puntuale nel quadro di ispezioni potrebbe essere il fatto delle medesime persone, purché riguardino settori cyber specifici. È tuttora aperto e sarà esaminato ulteriormente in quale misura i dipartimenti potrebbero coprire questo fabbisogno tramite un pool di esperti che concentrasse presso un servizio risorse specializzate aventi un medesimo grado specialistico di copertura e le mettesse a disposizione degli uffici specializzati.

La strategia ha ampliato il mandato di base di MELANI (DDPS e DFF) nel senso che nel quadro dei lavori di attuazione questo servizio sarà tenuto a fornire ulteriori prestazioni in ambito di quadro della situazione, di sostegno e di elaborazione di incidenti e di sostegno nell'analisi dei rischi e delle vulnerabilità presso i gestori di IC. I fornitori di prestazioni TIC e i fornitori di sistemi dovranno inoltre essere più fortemente coinvolti da MELANI. MELANI svolge quindi un ruolo centrale nell'attuazione delle misure della strategia, nel senso che questo servizio assume il coordinamento, la valutazione e la trasmissione del flusso di informazioni nel contesto della lotta conto i cyber-rischi informatici e garantisce lo scambio di informazioni con i gestori di IC, i fornitori rilevanti di prestazioni TIC e i fornitori di sistemi. Questa piattaforma informativa da ampliare costituisce il cuore della strategia. A fine 2017, alla conclusione dei lavori di attuazione, MELANI assumerà se del caso una funzione di coordinamento e di guida all'interno del proprio mandato. I compiti di MELANI sono pertanto documentati separatamente nella tabella qui appresso:

Dipartimenti	Nuovi posti	Riduzione fino a fine 2017	Attuazione delle seguenti misure della SNPC
DFAE	+2	0	7;8;9;10;11;13
DFGP	+1	-1	4;6;13;14
DDPS	+17	0	2;3;4;5;6;11;12;13;14
DFF	+6	-1	2;3;4;5; 6;7;8;9;10;11;12;13;14;16
DEFR	+2	0	2;12;13
DATEC	+2	0	2;3;7;8;9;10;11;12
Totale	+30	-2	
MELANI (risorse già documentate in DFF + DDPS)	+6	0	2;3;4;5;6;10;11;12;13;14

3.2 Rilevanza dei settori, dei settori parziali e dei gestori di IC

La Confederazione da sola può rafforzare soltanto limitatamente la cyber-resilienza nazionale. Le uscite documentate della Confederazione sono destinate a istituire condizioni quadro ottimali in vista di un'accresciuta cyber-resilienza nazionale. La collaborazione dei settori e dei settori parziali critici dell'economia e dei corrispondenti gestori di infrastrutture critiche costituiscono una parte importante dell'attuazione delle misure della strategia. È pertanto necessaria la riuscita del loro coinvolgimento nelle misure corrispondenti da parte degli uffici federali competenti mediante processi adeguati di informazione e di consultazione. I punti di riferimento riguardo alla ripartizione delle competenze sono reperibili nella Strategia PIC.

3.3 Sussidiarietà dell'esercito

Sebbene la SNPC escluda esplicitamente il caso di guerra e di conflitto e affidi all'esercito il compito di prepararsi in vista di questi casi speciali, l'esercito dispone di conoscenze essenziali, soprattutto sugli aspetti tecnici in ambito di cyber-rischi. Gli uffici responsabili dovrebbero se del caso integrare queste disponibilità di capacità nei loro processi di attuazione e attivarle all'occorrenza. Ciò corrisponde all'approccio affermato della sussidiarietà del ricorso all'esercito, ad esempio in caso di catastrofi naturali. In questo senso nel corso di una prima fase occorre istituire o ampliare presso gli uffici responsabili dell'attuazione della SNPC le conoscenze e le capacità in ambito di rischi informatici che consentono di ricorrere alle conoscenze e alle capacità dell'esercito in maniera orientata sulla soluzione e sull'obiettivo. Un coordinamento precoce con l'attuazione della SNPC significa quindi che in questo ambito possono essere individuate e sfruttate sinergie. Un coinvolgimento precoce è altresì destinato a porre in sintonia con il sistema globale Svizzera il concetto di cyber-difesa che deve essere elaborato dall'esercito.

3.4 Rischi di progetto nell’attuazione della SNPC

Esistono alcuni rischi da prendere in considerazione nell’attuazione della strategia. Uno dei più importanti è che le misure di attuazione non intervengano tempestivamente. Altri rischi sono:

- i rischi che insorgono per il fatto della mancanza di conoscenze dei singoli attori, come pure il subentro di incidenti sui quali l’attuazione della strategia interviene troppo tardi, rendendola in tal modo obsoleta agli occhi del pubblico;
- il coinvolgimento dei settori e dei settori parziali, come pure dei gestori di IC da parte degli uffici interviene troppo tardi o in maniera insufficiente, circostanza che potrebbe pregiudicare l’analisi dei rischi e delle vulnerabilità, nonché la gestione della continuità;
- la cooperazione è pregiudicata da una comunicazione insufficiente e da false aspettative da parte dei settori, dei settori parziali e dei gestori di IC;
- il mancato accantonamento delle risorse necessarie pregiudica l’attuazione delle misure in tutti gli ambiti della strategia;
- consecutivamente all’attuazione della strategia alcune infrastrutture critiche potrebbero fare emergere una necessità di intervento, ciò che significa ancora una volta l’insorgere di determinati costi per porre mano ai rischi corrispondenti.

4 Organizzazione di attuazione della SNPC

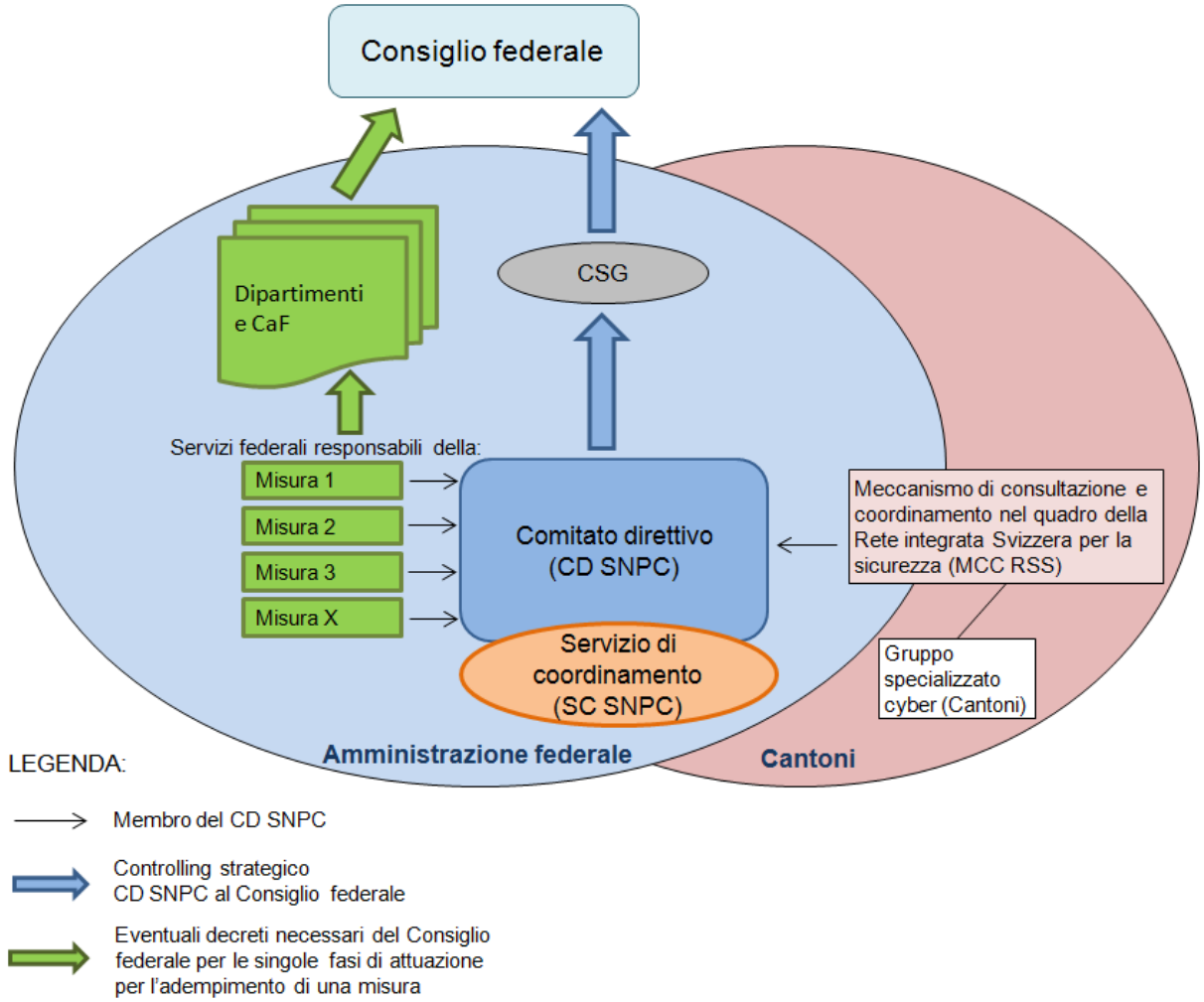

Figura 2: Organizzazione per l'attuazione della SNPC

4.1 Comitato direttivo della SNPC

Il Comitato direttivo della SNPC garantisce su incarico del Consiglio federale l'attuazione coordinata e orientata sugli obiettivi della SNPC (cfr. figura 2).

Esso ha le seguenti competenze e funzioni:

- verifica mediante controlling strategico il progresso conforme agli obiettivi e alle scadenze del portafoglio di misure della strategia e ne presenta rendiconto al Consiglio federale per il tramite della CSG;
- provvede a un modo di procedere coordinato presso i dipartimenti competenti a livello di attuazione delle misure, in particolare se tali misure toccano l'ambito della legislazione;
- sostiene attivamente la collaborazione dei servizi della Confederazione con i servizi rilevanti dei Cantoni, dell'economia e della società civile;

- garantisce che nel quadro delle attività di attuazione si prendano in considerazione la politica della Confederazione in materia di rischi, la SNPC e la Strategia del Consiglio federale per una società dell'informazione in Svizzera;
- verifica unitamente ai servizi competenti le possibilità di sinergia, come pure una semplificazione e uno snellimento dei sistemi e dei percorsi di comunicazione;
- segue l'evoluzione dei cyber-rischi e sottopone al Consiglio federale raccomandazioni corrispondenti in vista dello sviluppo ulteriore della strategia;
- presenta ogni anno al Consiglio federale, per il tramite del DFF, un rapporto sullo stato di attuazione della strategia che alla fine del 2017 assumerà la forma di un rapporto finale completo, corredato da un esame dell'efficacia della strategia e del suo piano d'attuazione. L'esame dell'efficacia sarà sottoposto al Consiglio federale già nella primavera del 2017.

Nel Comitato direttivo sono rappresentati tutti i dipartimenti sono responsabili di almeno una misura di attuazione. Vi è pure rappresentato il MCC RSS. La presidenza del Comitato direttivo è assunta dal DFF.

4.2 Servizio di coordinamento della SNPC

Il Servizio di coordinamento SNPC coordina l'attuazione della strategia a livello operativo e specialistico.

Esso ha i seguenti compiti:

- osserva e valuta sistematicamente i progressi dei lavori di attuazione della strategia e ne informa il Comitato direttivo;
- coordina e sostiene le attività di attuazione dei servizi responsabili ed esegue le misure che gli sono attribuite;
- individua e sfrutta le sinergie tra le misure di attuazione;
- organizza la collaborazione tra esperti interni ed esterni alla Confederazione, come pure con le loro organizzazioni;
- segue a livello nazionale e a livello internazionale, d'intesa con il Dipartimento federale degli affari esteri (DFAE), l'evoluzione e l'attuazione in ambito di cyber-strategie e comunica tempestivamente ai partner di attuazione rilevanti le informazioni che ne ha tratto;
- indice ogni anno una manifestazione per gli esperti SNPC nel quadro della quale i partner di attuazione possono creare nuovi contatti a livello nazionale, informarsi e scambiarsi informazioni.

4.3 Gruppi specializzati Cyber (GS-C) e Cyber internazionale (GS-CI)

Per coordinare i lavori con le interfacce sui Cantoni, il MCC RSS istituisce il gruppo specializzato Cyber (GS-C), composto di rappresentanti dei livelli Confederazione, Cantoni e Comuni.

Il GS-C coordina l'attuazione della SNPC a livello cantonale. Esso ha i seguenti compiti:

- coinvolge i Cantoni come partner costituzionali centrali in tutte le misure di attuazione che li riguardano;
- dirige i progetti parziali sotto forma di gruppi di lavoro nei settori «rafforzamento della resilienza», «incident handling» e «gestione delle crisi»;
- coordina l'attuazione dei progetti parziali cantonali e verifica mediante il controlling strategico i progressi conformi agli obiettivi e alle scadenze;
- garantisce lo stato completo delle conoscenze del gruppo specializzato sulle attività di attuazione della Confederazione nel quadro della strategia SNPC e promuove lo scambio di esperienze tra i membri del gruppo specializzato.

Il Servizio di coordinamento del SNPC è membro del gruppo specializzato cyber del MCC RSS e costituisce, a livello di Confederazione, il ponte con i progetti del gruppo specializzato cyber per sfruttare in maniera ottimale le sinergie ed evitare le ridondanze.

È inoltre previsto un gruppo specializzato Cyber internazionale (GS-CI) sotto la direzione del DFAE. L'obiettivo del GS-CI è di garantire il flusso dell'informazione in stretta cooperazione/collaborazione tra tutti i partecipanti. Il DFAE inviterà a una seduta costituiva tutte le parti interessate alla collaborazione internazionale nel settore cyber. In occasione di questo primo incontro si dovrà discutere in qual modo possa essere di ausilio ai partecipanti un gruppo interdipartimentale di lavoro esclusivamente dedito agli aspetti internazionali delle tematiche.

5 Misure e responsabilità

I sette settori di intervento e le loro relative misure strategiche (M1-M16) possono essere compendiati nei seguenti ambiti in funzione del loro dispiego nel tempo e delle loro dipendenze:

- **misure in ambito di prevenzione;**
- **misure in ambito di reazione;**
- **misure in ambito di gestione della continuità e della crisi;**
- **misure in ambito di processi di sostegno.**

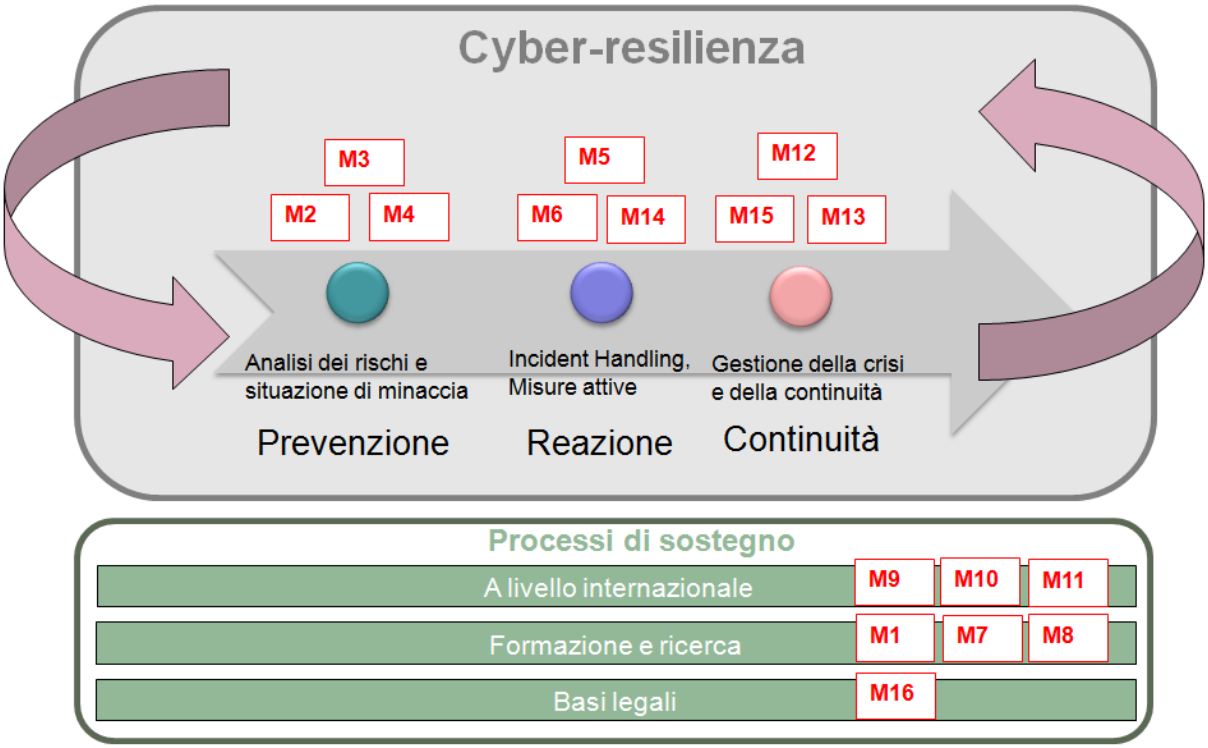

Figura 3: Le misure della strategia e le loro dipendenze in sintesi

La cyber-resilienza consta di processi ricorrenti di prevenzione, reazione e continuità. Il processo riprende da capo dopo la gestione della crisi in caso di evento.

Le informazioni tratte dai colloqui con i partner intervistati sono presentate nel prossimo capitolo, strutturate per ambiti e misure, come pure per responsabilità, competenze, obiettivi di attuazione e termini di consegna.

5.1 Misure in ambito di prevenzione

In ambito di prevenzione l'approccio di gestione globale della crisi della strategia PIC va applicato anche ai cyber-rischi ai sensi della presente strategia. Gli uffici responsabili dell'attuazione dispongono l'esecuzione di un'analisi dei rischi e delle vulnerabilità. Ciò viene effettuato anzitutto sotto la direzione dell'UFAE e delle autorità e dei regolatori competenti.

Per quanto riguarda la rappresentazione della situazione di minaccia è indispensabile riunire informazioni tecniche e non tecniche per analizzare e valutare in maniera completa i cyber-rischi. Queste informazioni sono messe a disposizione da MELANI. Per questo motivo MELANI va ampliata come piattaforma di informazione dei Cantoni e dei gestori di IC.

Si può presumere che la maggior parte dei settori critici, come pure i settori parziali e i corrispondenti gestori di infrastrutture critiche abbiano istituzionalizzato un'analisi dei rischi e delle vulnerabilità. In considerazione dell'aumento della minaccia la strategia deve fare sì che l'aspetto cyber sia preso esplicitamente in considerazione in un'analisi globale dei rischi. La strategia raccomanda di perseguire al riguardo un approccio uniforme e di riunire i risultati consolidati sotto forma di quadro della situazione con possibilità di evoluzione della situazione.

Questo approccio è parimenti destinato a garantire che i cyber-rischi siano documentati in maniera trasparente, specialmente nel caso dei piccoli gestori di IC. Così facendo è possibile illustrare in maniera ricostruibile – sulla base di considerazioni nazionali sovraordinate – i rischi residui inaccettabili e i costi della necessità di intervento identificata.

Campo d'azione 2	**Competenze: UFAE, UFPP, autorità specializzate/regolatori;** MELANI	**Misura 2**
Analisi dei rischi e delle vulnerabilità	L'UFAE elabora le analisi dei rischi e della vulnerabilità coadiuvato dai settori, dai settori parziali e dai gestori di IC. I settori e i settori parziali che non sono ancora rilevati dall'UFAE devono essere iniziati dall'UFPP, con il coinvolgimento delle autorità specializzate competenti. Esiste una chiara ripartizione di competenze tra UFAE e UFPP in merito alle responsabilità sui settori parziali.	Verifica autonoma dei sistemi Analisi per minimizzare i rischi in collaborazione con le autorità, i fornitori di prestazioni TIC e di sistemi.

Attuazione:

L'UFAE[3] e l'UFPP[4] sono di volta in volta responsabili dell'allestimento di un'analisi dei rischi e delle vulnerabilità dei settori parziali loro attribuiti. Ove possibile e opportuno il modo di procedere e la metodologia dovranno essere stabiliti d'intesa tra l'UFAE e l'UFPP. I settori e i settori parziali che non sono stati rilevati né dall'UFAE, né dall'UFPP, dovranno essere iniziati coinvolgendo le autorità specializzate corrispondenti (regolatori responsabili). Nella misura del possibile va anche seguito un approccio uniforme. I lavori dovranno essere conclusi a fine 2017.

Il consolidamento dei risultati sotto forma di analisi complessiva della situazione di minaccia è effettuato in collaborazione con MELANI.

[3] Cfr. nota a piè di pagina 1.
[4] Cfr. nota a piè di pagina 2.

Campo d'azione 2	**Competenze: ODIC;** UFIT, BAC, MELANI	**Misura 3**
Analisi dei rischi e delle vulnerabilità	L'ODIC allestisce un piano di verifica coadiuvato dai fornitori di prestazioni TIC. Il piano può servire da complemento al manuale PIC in ambito informatico. MELANI garantisce lo scambio con i gestori di IC, i fornitori di prestazioni TIC e i fornitori di sistemi.	L'infrastruttura TIC deve essere esaminata quanto alla presenza di vulnerabilità sistemiche, organizzative e tecniche: le autorità, i gestori di IC e le istituzioni di ricerca ricercano le vulnerabilità delle loro infrastrutture TIC coinvolgendo i fornitori di prestazioni TIC e di sistemi. Rientrano nelle vulnerabilità i punti deboli sistemici, organizzativi e tecnici.

Attuazione:

La SEC-ODIC allestisce entro il 2015 un piano di verifica che verrà attuato dai pertinenti fornitori di prestazioni e dai singoli responsabili delle segreterie generali dei dipartimenti. L'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e la Base d'aiuto alla condotta (BAC) sostengono questo concetto di verifica in quanto fornitori di prestazioni. Questo piano di verifica può essere rilasciato come raccomandazione all'economia e ai gestori di IC. Esso può inoltre essere presentato ai Cantoni dal gruppo specializzato Cyber del MCC RSS e fungere quindi da raccomandazione e sostegno alle proprie verifiche.

Il piano di verifica è coordinato con i progetti in corso, come ad esempio l'Information Security Management Systems (ISMS) della sicurezza dell'informazione e dell'oggetto (IOS).

Il consolidamento dei risultati sotto forma di analisi complessiva della situazione di minaccia è effettuato in collaborazione con MELANI.

Campo d'azione 3	**Competenze: MELANI, SIC, SCOCI;** BAC, SIC, UFIT	**Misura 4**
Analisi della situazione di minaccia	Ci si procurano da fonti pubbliche e non pubbliche informazioni di intelligence, di polizia, forensi e tecniche sulla situazione di minaccia e di rischio nel settore informatico. Questa misura è attuata nel quadro di diversi progetti posti sotto le direzione di diversi responsabili. MELANI genera in stretta collaborazione con il SIC e con fedpol/ SCOCI un'immagine della situazione attuale di minaccia. Il Servizio informazioni (SIC) adempie l'aspetto cyber del proprio mandato. CERTs: ampliamento delle capacità tecniche in vista della sorveglianza costante (24/7): CSIRT-UFIT, SIC-CSIRT, GovCERT.	Allestimento del quadro della situazione e dell'evoluzione della situazione.

Attuazione:

MELANI: allestimento (entro fine 2013) e attuazione (dal 2014) di un piano di rafforzamento di MELANI come piattaforma di scambio di informazioni. MELANI amplia la collaborazione sistematica con fornitori rilevanti di prestazioni TIC e con fornitori di sistemi. Maggiore scambio di informazioni con i gestori di IC e con l'economia.

SIC: costituzione di conoscenze specialistiche e di capacità nel settore cyber presso il SIC, con il COE-BAC e il servizio informazioni militare (SIM) come fornitori di prestazioni al SIC (2014–2015).

Le capacità tecniche di sorveglianza costante (24/7) delle reti della Confederazione vanno ampliate entro la fine del 2015.

- CERTs: MELANI: ampliamento di GovCERT per accrescere la capacità di resistenza (2014–2016)
- UFIT**:** ampliamento del CSIRT per accrescere la capacità di detenzione

5.2 Misure in ambito di reazione

Le misure in ambito di SNPC rilevanti ai fini dell'«incident handling» e dell'«incident response» servono a rafforzare i compiti e le capacità esistenti che contribuiscono alla cyber-resilienza e che non possono essere assunte da singoli attori. A seconda della circostanze nel contesto dell'«incident handling» e dell'«incident response» può anche insorgere la necessità di contromisure mirate e attive. In quale misura la Svizzera sia poi in grado di adottare all'estero misure attive al di sotto della soglia bellica va stabilito in definitiva nel processo di decisione politica.

Ambito di interveto 3	**Competenze: MELANI, SIC;** BAC, SIM, UFIT	**Misura 5**
Analisi della situazione di minaccia	La Confederazione, i Cantoni e i gestori di IC devono rielaborare gli eventi rilevanti ed esaminare le possibilità di sviluppo ulteriore di misure proprie in ambito di eventi inerenti ai cyber-rischi. MELANI raccoglie, valuta e analizza le informazioni e le mette a disposizione degli attori rilevanti (modello PPP). Mandato SIC, come per M4.	Rielaborazione di eventi in vista dello sviluppo ulteriore di misure.
Attuazione: Come nel caso di M4. UFIT: ampliamento delle capacità tecniche (incremento della possibilità di reazione a un incident) in direzione di una sorveglianza 24/7. L'ampliamento del CSIRT-UFIT per rafforzare le capacità tecniche e la capacità di resistenza deve essere effettuato entro il 2014. M4 potrà essere sostenuto grazie a questo ampliamento.		

Campo d'azione 3	**Competenze: SCOCI;** MELANI	**Misura 6**
Analisi della situazione di minaccia	La responsabilità immediata del perseguimento penale di cyber-incidenti compete ai Cantoni.	Casistica e coordinamento di complessi casi intercantonali.

Attuazione:

Fedpol elabora con il coinvolgimento dei Cantoni un piano per l'allestimento di una casistica globale (casi penali) e di coordinamento di casi intercantonali complessi. Il piano passerà al vaglio di due procedure di consultazione nei Cantoni ed è stato approvato dalla Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia. Il coordinamento all'interno di fedpol è assunto da SCOCI. Il piano rivolge un'attenzione speciale a progetti tra Confederazione e Cantoni già esistenti (ad es. Armonizzazione dell'informatica dei corpi di polizia in Svizzera AIP; "PICAR" per la creazione di un prospetto dei casi criminali di effrazione). Nel secondo trimestre del 2013 dovrà essere definito un gruppo centrale dell'organizzazione di progetto. Esso consterà di rappresentanti di:

Fedpol, CDDGP, Conferenza delle autorità inquirenti svizzere (CAIS), Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS), capo della AG IT della CCPCS, rappresentanti di Swiss Police ICT, un rappresentante del Ministero pubblico della Confederazione (MPC) e dell'Ufficio federale di giustizia (UFG).

Le procedure di consultazione si svolgeranno rispettivamente nel primo e nel secondo trimestre del 2014. Il piano dovrà essere allestito entro il terzo trimestre del 2015 e approvato dalla CDDGP. Nel quarto trimestre del 2015 si svolgerà la consultazione degli uffici. I preparativi di realizzazione seguiranno nel 2016.

A livello internazionale Europol e Interpol sono attori determinanti con i quali si dovrà coordinare il piano.

Le informazioni fornite dalla casistica (casi penali) e le informazioni fornite dai casi complessi nel contesto dell'analisi tecnico-operativa del perseguimento penale confluiscono per il tramite di MELANI in un'analisi complessiva della situazione di minaccia.

Campo d'azione 6	**Competenze: SIC, MELANI;** SCOCI, SIM	**Misura 14**
Gestione della continuità e della crisi	Il SIC è in linea di massima responsabile del reperimento di informazioni con le risorse dell'intelligence, della loro analisi e valutazione, al fine di diffonderne i risultati. Esso istituisce con il coinvolgimento della BAC quale fornitore tecnico di prestazioni e del SIM quale collegamento con il servizio di informazione militare, le capacità di effettuare l'identificazione degli autori e prepara misure attive corrispondenti nell'ipotesi dell'opportunità politica. Nel perseguimento penale e nell'identificazione degli autori svolge inoltre un ruolo importante lo SCOCI, coinvolto in eguale misura.	Misure attive di identificazione degli autori. Quando riesce a identificare gli autori il SIC trasmette le informazioni corrispondenti al Ministero pubblico della Confederazione, sempreché ciò sia legale. Il Ministero pubblico decide se intende avviare una procedura penale. Se il perseguimento penale non è opportuno o possibile occorre preparare contromisure attive. La base legale corrispondente va prevista nella LSI.

Attuazione:

Adeguamento entro la fine del 2013 SLA (service level agreement) con il COE-BAC. Costituzione di conoscenze specialistiche presso il SIC unitamente al COE-BAC e al SIM come fornitori di prestazioni (2014–2015).

Le informazioni tratte dall'analisi della situazione di minaccia da parte di MELANI e le possibilità di identificazione e di dimostrazione della colpevolezza degli autori insite nell'ambito del mandato legale di perseguimento penale confluiscono nelle misure.

5.3 Misure in ambito di gestione della continuità e della crisi

Dallo Stato ci si aspetta che esso disponga delle risorse che gli consentono di sostenere a titolo sussidiario i servizi responsabili, se questi ultimi non sono più in grado di adottare autonomamente le misure necessarie. Unitamente ai suoi co-fornitori (in particolare il SIC), MELANI fornisce un simile sostegno nel quadro del CUG (cerchia chiusa della clientela di MELANI). Queste prestazioni vanno stabilite in tutti i settori e settori parziali nonché presso i gestori di infrastrutture critiche.

I processi di analisi degli incident e di gestione della continuità e della crisi devono essere armonizzati tra di loro. La crisi è generalmente provocata da un incident, ma non ogni incident si trasforma in una crisi. Occorre pertanto un'escalation dall'«incident handling» alla gestione della crisi. I piani di gestione della crisi rientrano nella gestione della continuità. Spetta quindi agli uffici competenti nonché alle autorità specializzate competenti e ai regolatori provvedere affinché i settori, i settori parziali e i gerenti corrispondenti di infrastrutture critiche dispongano nel loro ambito di responsabilità di un «incident handling» funzionante e di una gestione della crisi.

Campo d'azione 6	**Competenze: UFAE, UFPP, autorità specializzate/regolatori;** MELANI	**Misura 12**
Gestione della continuità e della crisi	In ambito di gestione della continuità le competenze sono identiche a quelle indicate in M2.	Rafforzamento e miglioramento della capacità di resistenza (resilienza) nei confronti di perturbazioni e di eventi.
Attuazione: L'attuazione della gestione della continuità è identica a quella indicata in M2. Al riguardo il DEFR adegua le proprie competenze nel quadro della revisione della LAP. La gestione della continuità è un processo in corso. Esso si fonda sulle analisi esistenti di rischio e di vulnerabilità e può pertanto essere eseguito soltanto quando M2 è portata a termine. MELANI sostiene e rafforza lo scambio volontario e reciproco di informazioni con i gerenti di IC, i fornitori di prestazioni TIC e i fornitori di sistemi al fine di sostenere la continuità e la capacità di resistenza sulla base dell'autoaiuto. Ciò comporta un fabbisogno accresciuto di capacità forensi e un flusso crescente di informazioni.		

Campo d'azione 6	**Competenze: UFAE, MELANI, UFPP;** SCOCI, DFAE, autorità specializzate/regolatori	**Misura 13**
Gestione della continuità e della crisi	In ambito di gestione della crisi le competenze sono identiche a quelle indicate in M2 e M12. MELANI assume la parte operativa e, in caso di crisi, garantisce un sostegno sussidiario agli attori interessati, mettendo a disposizioni conoscenze esperte. Per garantire il perseguimento penale, viene strettamente coinvolto il fedpol / SCOCI. Nei casi in cui si presentano possibili implicazioni di politica estera, occorre informare il più rapidamente possibile il DFAE e coinvolgerlo nell'elaborazione di corrispondenti piani previdenziali. Gli uffici responsabili si coordinano e accordano tra di loro.	Coordinamento delle attività, in primo luogo con gli attori direttamente interessati nonché sostegno ai processi di ricerca di soluzioni con perizie specializzate.

Attuazione:

L'attuazione della gestione della crisi è identica a quella indicata M12. Al riguardo il DEFR propone un adeguamento delle proprie competenze nel quadro della revisione della LAP. La gestione della crisi è un processo continuo. Esso si fonda sulle analisi esistenti di rischio e di vulnerabilità e può pertanto essere eseguito soltanto alla loro conclusione.

Nel quadro di MELANI e dei suoi partner appartenenti alla cerchia chiusa della clientela, esistono processi funzionanti per affrontare l'escalation degli incident in collaborazione con le esistenti organizzazioni di crisi dell'amministrazione e dell'economia.

Per poter garantire un modo di procedere uniforme e paragonabile e utilizzare al meglio i contatti stabiliti, è importante disporre di una procedura coordinata tra UFAE e UFPP.

Campo d'azione 6	Competenze: CaF	Misura 15
Gestione della continuità e della crisi	Occorre elaborare sotto la responsabilità della Cancelleria federale (CaF) un piano sugli iter di condotta e di processo, in vista di una soluzione tempestiva del problema che tenga anche conto degli aspetti cyber.	Elaborazione di un piano sugli iter di condotta e di processo in vista di una soluzione tempestiva del problema.
Attuazione: La gestione (generale) della crisi deve essere adeguata e comprendere anche l'aspetto cyber. Gli iter di condotta e di processo della Confederazione tengono conto dell'aspetto cyber all'interno dei processi esistenti. Occorre elaborare sotto la responsabilità della CaF il piano sugli iter di condotta e di processo, in vista di una soluzione tempestiva del problema che tenga anche conto dell'aspetto cyber.		

5.4 Processi di sostegno

Dato che la protezione delle infrastrutture di informazione e comunicazione contri i cyber-rischi è di interesse nazionale per la Svizzera, occorre altresì creare le basi necessarie. Rientrano in tal ambito:

- la verifica della conformità delle basi legali esistenti alle misure di protezione;
- le cooperazioni e gli sforzi internazionali volti a tutelare il cyberspazio dagli abusi mediante norme e standard convenuti a livello internazionale;
- lo scambio di esperienze, di lavori di ricerca e sviluppo, di informazioni riferite agli eventi e di attività di formazione ed esercizio;
- la collaborazione della Svizzera nel quadro di organizzazioni internazionali statali e non statali, al fine di ridurre i cyber-rischi.

Per poter accrescere la cyber-resilienza, nei propri ambiti di responsabilità occorre disporre delle capacità di identificazione, valutazione e analisi dei rischi in relazione alla problematica cyber. Al riguardo la strategia incarica gli uffici federali competenti di attuare le seguenti misure che devono essere in parte avviate in collaborazione con i servizi competenti dei Cantoni. Per rafforzare la cyber-resilienza i Cantoni e i gestori di IC devono poter fondarsi su queste basi, dato che si tratta di compiti statali che non possono essere assunti dai singoli attori.

Campo d'azione 1	Competenze: servizi federali responsabili	Misura 1
Identificazione dei rischi attraverso la ricerca	Saranno concretizzati nel corso delle ulteriori attuazioni.	Occorre effettuare ricerche sui nuovi rischi in relazione alla problematica cyber.

Attuazione

Le lacune di conoscenza e capacità nel settore cyber possono essere identificate dai gruppi di interlocutori seguenti:

- CERTs;
- gestori di IC;
- offerenti di TIC.

I servizi seguenti conducono progetti/programmi di Cyber-Research:

- UE;
- sezioni dei PF;
- università e Scuole universitarie professionali;
- laboratori di ricerca TIC (ad es. IBM).

Campo d'azione 4	Competenze: SC SNPC; UFCOM, DFAE, UFAS	Misura 7
Formazione delle competenze	Il Servizio di coordinamento della SNPC elabora in collaborazione con l'UFAS (programma gioventù e media)[5], il DFAE e l'UFCOM un prospetto delle offerte di formazione delle competenze. Il prospetto è elaborato in coordinamento con i lavori di attuazione della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e i Cantoni. Il DFAE fornisce informazioni sulle offerte nel quadro delle organizzazioni e istituzioni internazionali.	Creazione di un prospetto delle offerte di formazione delle competenze.

Attuazione:

Il prospetto delle offerte di formazione delle competenze deve essere allestito entro la fine del 2013, mentre le offerte di formazione delle competenze devono essere pubblicate entro la metà del 2014.

[5] DCF 11.06.2010, Programma nazionale per la protezione dell'infanzia e della gioventù dai rischi dei media e la promozione delle competenze mediali.

Campo d'azione 4	**Competenze: SC SNPC;** UFCOM, DFAE, UFAS	**Misura 8**
Formazione delle competenze	D'intesa con la «Strategia del Consiglio federale per una società dell'informazione in Svizzera», con i Cantoni e l'economia e in collaborazione con l'UFAS, il DFAE, l'UFCOM nonché con le autorità specializzate e i regolatori, il Servizio di coordinamento della SNPC coordina l'elaborazione di un piano di attuazione per una maggiore utilizzazione delle offerte esistenti e altamente qualitative volte a gestire i cyber-rischi e per la creazione di nuove offerte formali e informali di formazione delle competenze. Il DFAE fornisce informazioni sulle offerte nel quadro delle organizzazioni e istituzioni internazionali.	Colmare le lacune nell'ambito delle offerte di formazione delle competenze e maggiore utilizzazione delle offerte.
Attuazione: Entro la fine del 2015 occorre creare un piano di attuazione per una maggiore utilizzazione delle offerte esistenti volte a gestire i cyber-rischi nonché nuove offerte di formazione delle competenze.		

Campo d'azione 5	**Competenze: UFCOM; autorità specializzate/regolatori, DFAE, POLSIC, MELANI**	**Misura 9**
Relazioni e iniziative internazionali	L'UFCOM partecipa attivamente ai processi rilevanti internazionali in ambito di Internet Governance (in particolare ICANN, ITU, CSTD e IGF), identifica continuamente gli aspetti rilevanti ai fini della stabilità, della disponibilità e della sicurezza, coordina gli interessi svizzeri con i rappresentanti dell'amministrazione, dell'economia e della società civile e rappresenta tali interessi nei processi e nelle istituzioni menzionati.	Internet Governance: la Svizzera partecipa nella misura del possibile al coordinamento dell'Internet Governance e si adopera attivamente a favore di una Internet Governance compatibile con i principi svizzeri di libertà e di responsabilità (personale), di approvvigionamento di base, di pari opportunità, di diritti dell'uomo e di Stato di diritto.
Attuazione: L'UFCOM e il DFAE, con il coinvolgimento del DDPS per le questioni di politica di sicurezza (SG-DDPS/POLSIC) e in collaborazione con i dipartimenti coinvolti, elaborano entro la fine del 2013 un prospetto delle manifestazioni, iniziative e organismi internazionali prioritari con riferimento alla Internet Governance.		

Campo d'azione 5	**Competenze: DFAE;** POLSIC, MELANI, UFCOM	**Misura 10**
Relazioni e iniziative internazionali	Il DFAE deve avviare attività mirate in ambito di cooperazione internazionale. Una possibilità ipotizzabile è la creazione di un «Code of Conduct» in relazione all'aspetto cyber. L'obiettivo a lungo termine è stabilire norme vincolanti a livello di diritto internazionale. Si persegue inoltre l'idea di affermare/ampliare Ginevra come centro per le questioni su Internet. Nell'attuazione di questa misura, il DFAE sarà sostenuto da SG-DDPS/POLSIC.	Cooperazione a livello di politica internazionale di sicurezza, per affrontare la minaccia nel cyberspazio, in collaborazione con altri Stati e altre organizzazioni internazionali. Nel quadro della cooperazione internazionale devono essere avviate rispettivamente portate avanti attività mirate, affinché la Svizzera possa tutelare i propri interessi nei diversi organismi internazionali.
Attuazione: Entro la fine del 2013 deve essere elaborato un piano a medio termine, interno al DFAE, per attuare la SNPC in ambito di cooperazione internazionale. MELANI e l'UFCOM sostengono questo processo.		

Campo d'azione 5	**Competenze: SC SNPC ;** autorità specializzate/regolatori, DFAE, MELANI	**Misura 11**
Relazioni e iniziative internazionali	MELANI e le autorità specializzate come pure i regolatori, rafforzano lo scambio di informazioni su approcci e iniziative internazionali tra i gestori di IC, i fornitori di prestazioni TIC e i fornitori di sistemi. In tal modo MELANI e il DATEC sostengono il coinvolgimento della piazza economica Svizzera in questi organismi internazionali. Se auspicato, MELANI, il DATEC e il DFF garantiscono questa partecipazione d'intesa con i dipartimenti, in particolare con il DFAE.	Coordinamento degli attori in ambito di partecipazione a iniziative e best practices nel settore della sicurezza e dei processi di tutela. Nel quadro di iniziative private e statali, di conferenze e di processi di standardizzazione nel settore della sicurezza e della tutela, i gestori, le associazioni e le autorità si coordinano per accedere a questi organismi.
Attuazione: In una prima fase i partner coinvolti (autorità specializzate e regolatori) devono effettuare un inventario di chi deve in linea di massima partecipare a iniziative e organismi internazionali. In una seconda fase occorre procedere a un consolidamento. Al riguardo vengono coinvolti le autorità specializzate, l'industria e se del caso il DFAE. Il SC SNPC coordina questo processo.		

Campo d'azione 7	**Competenze: SC SNPC**	**Misura 16**
Basi legali	Unitamente ai dipartimenti competenti, l'ODIC gestisce il Servizio di coordinamento per l'attuazione della strategia. Per quanto riguarda le lacune legislative identificate come prioritarie e gli adeguamenti legali necessari, i dipartimenti competenti elaborano i progetti necessari ai livelli normativi corrispondenti.	Verifica delle basi legai esistenti.
Attuazione: Il Servizio di coordinamento della SNPC elabora entro la fine del 2013 un primo prospetto delle necessità urgenti di legislazione e di revisione nel settore cyber. Al più tardi entro la fine del 2014 è necessario sottoporre al Consiglio federale, unitamente a uno scadenzario, un piano di regolamentazione delle lacune legislative identificate come prioritarie.		

6 Allegato

Documenti referenziati

Titolo	Autore/ Editore	Data
[1] Strategia nazionale per la protezione della Svizzera contro i cyber-rischi	DDPS	19.06.2012
[2] Strategia nazionale per la protezione delle infrastrutture critiche	DDPS – UFPP	27.06.2012
[3] Manuale sulla protezione delle infrastrutture critiche	DDPS – UFPP	Disegno 23.07.2012
[4] Manuale sulla gestione dei rischi della Confederazione	DFF	Versione 1.0

Elenco dei partner intervistati

Uffici federali	Partecipanti	Data
UFAE - UFPP – ODIC (seduta di voto)	Ruedi Rytz (UFAE), Toni Lauber (UFAE), Stefan Brem (UFPP), Nick Wenger (UFPP), Pascal Lamia (ODIC), Stefanie Frey (ODIC), Franz Zingg (ODIC), Marc Henauer (SIC)	07.01.2013
BAC	Riccardo Sibilia, Gérald Vernez	11.01.2013
DFAE	Michele Coduri, Christoph Bühler	21.01.2013
fedpol-SCOCI	Roland Becker, Thomas Walther, Tobias Bolliger	11.01.2013
FINMA	Marc Sander	04.01.2013
GS-DDPS	Jürg Treichler	14.01.2013
MCC RSS	Bernhard Wigger, Dario Walder	14.01.2013
ODIC-MELANI	Pascal Lamia, Stefanie Frey	18.01.2013
SEC-ODIC	Marcel Frauenknecht, Franz Zingg, Daniel Graf	11.01.2013
SIC	Philipp Kronig, Reto Camenisch	17.01.2013
UFAC	Urs Haldimann	11.01.2013
UFAS	Thomas Vollmer	27.02.1013
UFCOM	Armin Blum	17.01.2013
UFE	Christian Holzner, Hans-Peter Binder	17.01.2013
UFIT	Heino Kronenberg	17.01.2013
UFT	Petra Breuer, Ulrich Schär, Heinz Geiser	14.01.2013

Abbreviazioni

Abbreviazione	Descrizione
BAC	Base d'aiuto alla condotta del DDPS
CAIS	Conferenza delle autorità inquirenti svizzere
CCPCS	Conferenza dei comandanti delle polizie cantonali della Svizzera
CD SNPC	Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
CDDGP	Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia
CERT	Computer Emergency Response Team
COE-BAC	Centro operazioni elettroniche della base d'aiuto alla condotta del DDPS
CSG	Conferenza dei segretari generali
CSIRT	Computer Security Incident Response Team
CUG	Closed User Group (elemento di MELANI)
FRT	Formazione, ricerca e tecnologia
Gestore IC	Gestore di infrastrutture critiche
GS-C	Gruppo specializzato cyber
LAP	Legge federale dell'8 ottobre 1982 sull'approvvigionamento economico del Paese (Legge sull'approvvigionamento del Paese, LAP)
MCC RSS	Meccanismo di consultazione e coordinamento nel quadro della Rete integrata Svizzera per la sicurezza
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
POLSIC	Settore Politica di sicurezza (unità del SG-DDPS)
SC SNPC	Servizio di coordinamento per l'attuazione della strategia
SCOCI	Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet presso il DFGP
SEC-ODIC	Sezione sicurezza informatica dell'Organo direzione informatica della Confederazione
SiLAN SIC	LAN di sicurezza del SIC
SIM	Servizio informazioni militare presso il DDPS
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SONIA	Stato maggiore speciale Information Assurance
Strategia PIC	Strategia nazionale per la protezione delle infrastrutture critiche
UFAS	Ufficio federale delle assicurazioni sociali
UFIT	Ufficio federale dell'informatica e della telecomunicazione presso il DFF