Rapporto sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022

Stato secondo trimestre 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

Indice

1 Stato di attuazione: quadro generale 4
2 Organizzazione e strategie parziali per l'attuazione della SNPC 5
2.1 NCSC 5
2.2 Strategia Ciber DDPS 6
2.3 Accordo amministrativo concernente la rete NEDIK 6
2.4 Strategia di politica estera digitale 7
3 Priorità tematiche nell'attuazione della SNPC 8
3.1 Creazione di un istituto nazionale di test per la cibersicurezza (NTC) 8
3.2 Marchio di qualità cyber-safe.ch per i Comuni svizzeri 9
3.3 Marchio di qualità per i fornitori di servizi IT 9
3.4 Campagna nazionale di sensibilizzazione 9
3.5 Progetto pilota con Bug Bounty Switzerland 10
3.6 Elaborazione di un avamprogetto sull'introduzione dell'obbligo di notifica di ciberattacchi 10
4 Lo stato di attuazione nel dettaglio 11
4.1 Campo d'azione 1 "acquisizione di conoscenze e competenze" 11
4.2 Campo d'azione 2 "situazione di minaccia" 13
4.3 Campo d'azione 3 "gestione della resilienza" 13
4.4 Campo d'azione 4 "standardizzazione / regolazione" 15
4.5 Campo d'azione 5 "Gestione degli incidenti" 16
4.6 Campo d'azione 6 "Gestione delle crisi" 18
4.7 Campo d'azione 7 "Perseguimento penale" 19
4.8 Campo d'azione 8 "Ciberdifesa" 20
4.9 Campo d'azione 9 "Posizionamento attivo della Svizzera nella politica di sicurezza informatica internazionale" 21
4.10 Campo d'azione 10 "Visibilità e sensibilizzazione" 22

Premessa

Dall'ultimo rapporto sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022 è trascorso poco più di un anno. Allora avevo riassunto dicendo «Siamo a buon punto». Lo siamo ancora, anche se avrei preferito essere un po' più avanti nell'attuazione. Nel frattempo sono trascorsi ben due terzi del tempo destinato all'attuazione e circa il 60 per cento delle tappe fondamentali sono state realizzate. Sarebbe ancora meglio – anche solo dal punto di vista matematico – se ne fossero già state attuate due terzi. Di fatto, però, la conclusione delle tappe fondamentali ancora in corso è previsto per la fine di quest'anno o a fine 2022, quindi allo scadere della SNPC.

Maggiore è l'eterogeneità di un progetto, tanto più importanti diventano il coordinamento e la creazione di strutture chiare. Per quanto riguarda l'attuazione della SNPC, la creazione di strutture organizzative in seno alla Confederazione è quindi un elemento centrale. L'entrata in vigore dell'ordinanza del 27 maggio 2020 sulla protezione contro i ciber-rischi nell'Amministrazione federale (OCiber; RS *120.73*) a metà del 2020 ha permesso di chiarire il quadro e le competenze e di regolamentare la collaborazione in seno all'Amministrazione federale e con i Cantoni, l'economia e gli ambienti scientifici.

Ritengo che l'attuazione della SNPC abbia acquisito uno slancio significativo nell'ultimo periodo in esame, compreso tra il secondo trimestre del 2020 e il secondo trimestre del 2021. Gli ambiti inerenti alla cibersicurezza, alla ciberdifesa e al perseguimento penale dei cibercriminali si sono evoluti sia dal punto di vista strategico, sia da quello organizzativo.

Lo sviluppo del Centro nazionale per la cibersicurezza (NCSC) è stato portato avanti e sono stati introdotti altri servizi. È in corso la creazione di un sistema di gestione delle vulnerabilità. In questo contesto è anche stato condotto con successo un progetto pilota in cui hacker etici sono stati incaricati di individuare vulnerabilità in alcuni sistemi dell'Amministrazione federale. In futuro, i cosiddetti «programmi bug bounty» verranno estesi a tutta l'Amministrazione federale. Nel quadro dell'app SwissCovid e del certificato COVID, l'NCSC ha condotto due test pubblici per la valutazione della sicurezza, mettendo a disposizione dell'Amministrazione federale le sue competenze specialistiche. In un «private security test» che ha preceduto i test pubblici dl certificato COVID è stato coinvolto per la prima volta l'Istituto Nazionale di Test per la Cibersicurezza (NTC), costituito su iniziativa del Cantone di Zugo.

Con la sua Strategia Ciber, il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) ha gettato le basi necessarie per definire l'orientamento strategico in ambito di ciberdifesa tramite. La Strategia Ciber mostra come il DDPS partecipa alla SNPC sovraordinata. Va inoltre menzionato l'avanzamento dei lavori per la creazione del Comando Ciber dell'esercito, che assumerà un ruolo importante nella ciberdifesa. Il DDPS ha anche già partecipato a diverse ciberesercitazioni e ne ha anche condotte alcune, sempre all'insegna dello spirito di cooperazione.

Nell'ambito del perseguimento penale, un accordo amministrativo ha permesso di disciplinare l'organizzazione e il finanziamento di una rete di supporto digitale alle indagini sulla criminalità informatica (NEDIK). La rete concentra le risorse specializzate a livello nazionale al fine di lottare in modo efficiente contro la criminalità informatica e contribuire alla prevenzione. Il dialogo strategico condotto tramite il Cyberboard tra il Ministero pubblico della Confederazione, fedpol e le autorità cantonali preposte alla sicurezza assume sempre più importanza per orientare il perseguimento penale al futuro in modo ottimale.

Resta ancora un anno e mezzo per attuare la SNPC. C'è ancora molto da fare, ma sono convinto che riusciremo a compiere rapidamente ulteriori progressi a vantaggio della popolazione, delle autorità, dell'economia e della scienza. Naturalmente le sfide e i lavori nell'ambito della cibersicurezza continueranno anche dopo la conclusione della SNPC 2018–2022: gli accertamenti e i lavori preliminari in vista della strategia successiva sono già stati avviati.

1 Stato di attuazione: quadro generale

Il piano di attuazione della SNPC prevede 275 tappe fondamentali, articolate in 29 misure. Nel secondo trimestre del 2021 sono state attuate 154 tappe fondamentali e 8 non sono state attuate. Ciò significa che sono state completate 6 delle 29 misure. Il quadro dettagliato dello stato di attuazione è descritto al numero 5. La panoramica sottostante illustra lo stato di attuazione a grandi linee e le tappe fondamentali previste.

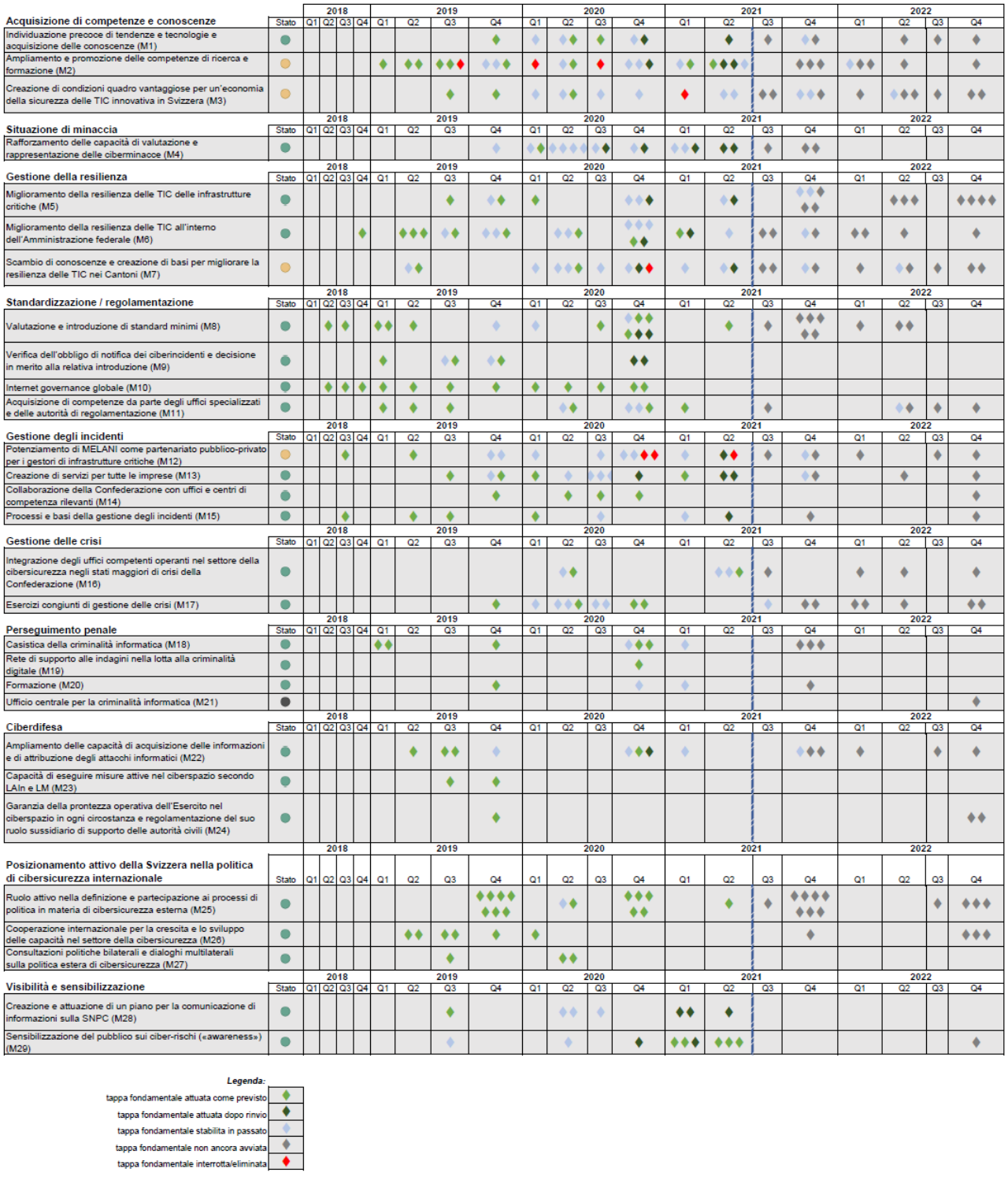


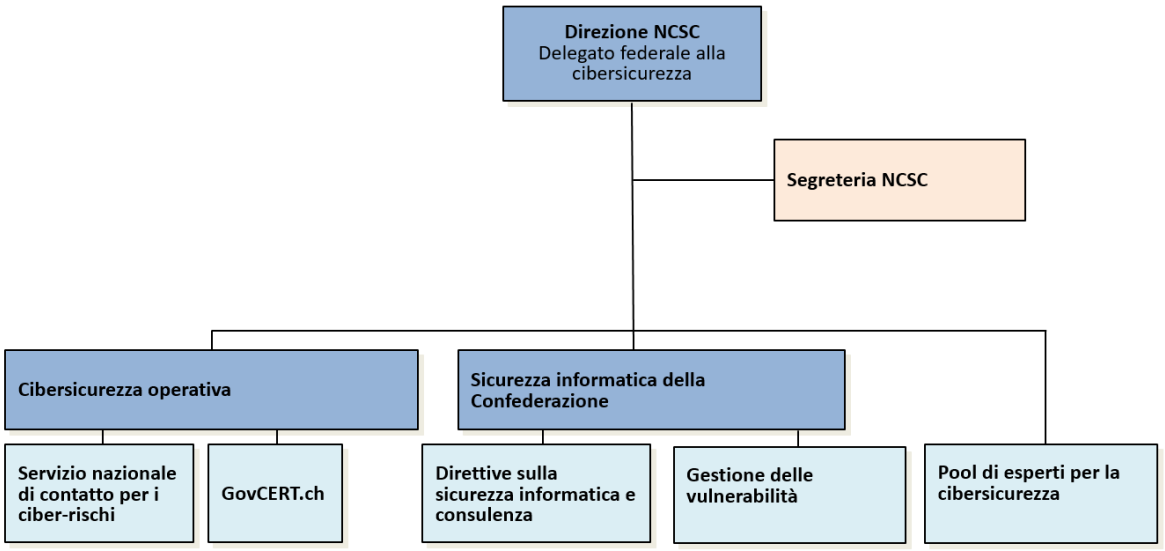
Figura 1: Panoramica dello stato di attuazione

2 Organizzazione e strategie parziali per l'attuazione della SNPC

La creazione di strutture organizzative in seno alla Confederazione è parte dell'attuazione della SNPC. Nel rapporto 2020 sullo stato di attuazione sono stati descritti gli organi di coordinamento sovradipartimentali (Comitato per la cibersicurezza del Consiglio federale, Comitato ristretto ciber e Comitato direttivo SNPC). Questi organi hanno proseguito il proprio lavoro e si sono incontrati regolarmente. Il presente rapporto verte sui principali sviluppi organizzativi e strategici in ambito di cibersicurezza, ciberdifesa e perseguimento penale della cibercriminalità.

2.1 NCSC

Nel corso del 2020 il potenziamento dell'NCSC è stata accelerata ulteriormente e il 13 maggio 2020 il Consiglio federale ha autorizzato la creazione di altri 11 posti. Nel maggio 2021 l'NCSC contava 32 collaboratori ed entro fine anno saranno occupati 13 posti ancora vacanti. L'organizzazione dell'NCSC è rappresentata nella figura 1.



Dal 1° gennaio 2020 l'NCSC offre un servizio di contatto nazionale per ciberincidenti. Nel primo anno di attività sono pervenute 10 834 segnalazioni da parte di imprese e popolazione. Per quanto riguarda le segnalazioni chiaramente ciber-rilevanti, si contano 5924 tentativi di frode (55 %), 416 casi di malware (4 %), 165 hackeraggi (2 %) e 24 casi riguardavano fughe di dati (<1 %).
GovCERT («Computer Emergency Response Team») è il team di analisi tecnica dell'NCSC. In collaborazione con i propri partner, nel 2020 ha bloccato 7500 pagine di phishing, registrato 4500 casi di malware informando 90 000 IP infetti e fornito a 177 gestori di infrastrutture critiche informazioni specifiche su minacce.
Nell'ambito delle disposizioni legali, le Istruzioni del Consiglio federale sulla sicurezza TIC nell'Amministrazione federale sono state trasposte nell'ordinanza sui ciber-rischi con effetto dal 1° aprile 2021, semplificando in tal modo le direttive e rafforzando il ruolo del delegato federale alla cibersicurezza. Ora il delegato può emanare direttamente delle direttive concernenti il processo e la documentazione della procedura di sicurezza.[1]

[1] https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/cyrv-vorgaben.html

2.2 Strategia Ciber DDPS

La Strategia Ciber DDPS, approvata dal capodipartimento nella primavera del 2021, costituisce la base per l'orientamento strategico nell'ambito della ciberdifesa per il periodo 2021–2024.[2] Essa mostra come il DDPS partecipa alla SNPC sovraordinata, contribuisce alla protezione della Svizzera, la difende nel ciberspazio e aumenta considerevolmente la sua libertà d'azione. Comprende tutte le misure militari e del Servizio delle attività informative che servono a proteggere i sistemi critici per la sicurezza nazionale, a respingere i ciberattacchi, a garantire l'efficienza operativa dell'Esercito in ogni situazione e a creare le capacità e le competenze per fornire un supporto sussidiario alle autorità civili.
Per l'attuazione vige il principio secondo cui tutti gli attori con compiti rilevanti in ambito ciber nel DDPS si coordinano attivamente nel quadro della Strategia Ciber DDPS. Lavorano insieme per identificare e gestire congiuntamente i rischi e le opportunità. Inoltre, il Dipartimento orienta il suo sviluppo sul piano specialistico, materiale, processuale come pure del personale in funzione delle sfide poste dalle ciberminacce. In questo contesto rivestono un'importanza fondamentale l'istruzione e il perfezionamento di tutti i collaboratori del DDPS nonché dei militari (personale di professione e di milizia).
Inoltre, per attuare le misure i responsabili dell'ambito ciber in seno al DDPS collaborano con i partner, ossia con l'NCSC, i Cantoni, i Comuni, la ricerca, l'economia privata, organizzazioni internazionali e alcuni Stati.

2.3 Accordo amministrativo concernente la rete NEDIK

Nella riunione autunnale del 12 novembre 2020, la Conferenza dei direttori cantonali di giustizia e polizia (CDCGP) ha approvato i termini di un accordo amministrativo stipulato con la Conferenza dei comandanti cantonali di polizia (CCPCS), che disciplina l'organizzazione e il finanziamento di una rete di supporto digitale alle indagini sulla criminalità informatica (NEDIK).[3] L'accordo è entrato in vigore il 1° gennaio 2021.
La rete NEDIK, istituita nel 2018 dalla CCPCS, mira a concentrare le risorse specializzate affinché la lotta contro la criminalità informatica possa essere condotta in modo efficiente. L'accordo amministrativo ha regolato l'organizzazione e il finanziamento di NEDIK.
NEDIK ha il compito, tra le altre cose, di garantire il reciproco trasferimento di conoscenze, di redigere una panoramica nazionale dei casi e di permettere la classificazione dei casi intercantonali. Inoltre NEDIK contribuisce alla prevenzione e collabora con la Prevenzione Svizzera della Criminalità (PSC) e l'NCSC.
In seno al NEDIK, fedpol assume il ruolo di coordinatrice sovracantonale e transnazionale, in particolare nella collaborazione con autorità partner all'estero. fedpol elabora pure i rapporti di analisi e rappresenta la Svizzera in seno a gruppi di esperti internazionali.

[2] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-83160.html

[3] https://www.kkjpd.ch/newsreader/verst%C3%A4rkter-einsatz-der-kantone-gegen-cyber-und-p%C3%A4dokriminalit%C3%A4t.html

2.4 Strategia di politica estera digitale

Nel novembre del 2020 il Consiglio federale ha adottato la Strategia di politica estera digitale.[4] Per quanto riguarda la cibersicurezza, la Strategia stabilisce la volontà della Svizzera di rafforzare la promozione della pace, ovunque possibile. Concretamente, nello spazio digitale questo significa favorire l'attuazione di strutture e spazi di scambio che permettano l'applicazione del diritto internazionale e del diritto internazionale umanitario. La Svizzera riconosce la validità delle norme in vigore e intende applicarle nella lotta contro ogni forma di ciberattacco. La cibersicurezza coinvolge una serie di attori che vanno dallo Stato alla società civile, passando per gli operatori economici. L'approccio «multistakeholder» è una costante nella definizione strategica della politica estera svizzera, così come lo è la sua lunga tradizione in materia di buoni uffici.

[4] https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_IT.pdf

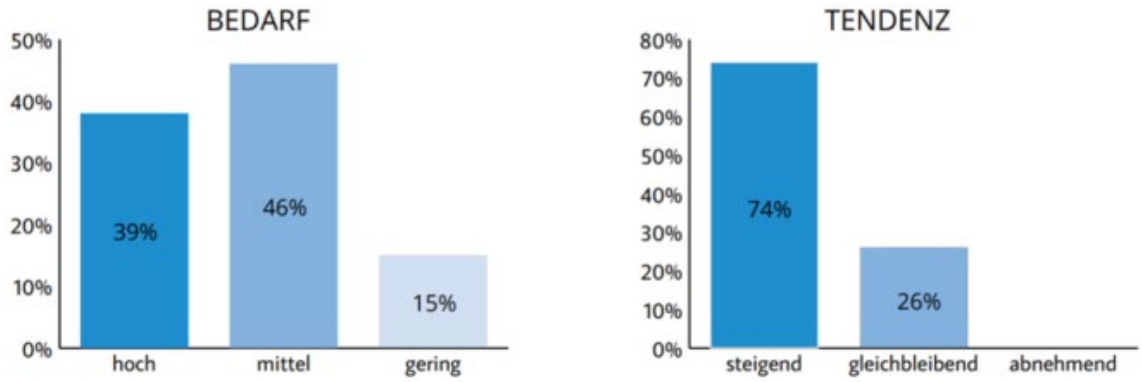
3 Priorità tematiche nell'attuazione della SNPC

I lavori di attuazione della SNPC proseguono di pari passo con l'ulteriore implementazione dell'organizzazione della cibersicurezza della Confederazione. Questa strategia non è portata avanti solo dall'Amministrazione federale, bensì sostenuta in modo significativo dai Cantoni, dalle università e più in generale dalla società. Mentre al numero 5 sono presentate le tappe fondamentali attuate nei singoli campi d'azione, il numero 3 è incentrato sui progetti chiave dei lavori in corso.

3.1 Creazione di un istituto nazionale di test per la cibersicurezza (NTC)

La sicurezza dei prodotti digitali è fondamentale per la cibersicurezza. Se i prodotti contengono vulnerabilità, sussiste una minaccia reale con un notevole potenziale di danno per l'economia e la società, soprattutto se vengono impiegati da infrastrutture critiche. Tuttavia, la Svizzera non disponeva di capacità sufficienti per testare questi prodotti e individuare eventuali vulnerabilità.
Su iniziativa del Cantone di Zugo è stato pertanto fondato l'Istituto Nazionale di Test per la Cibersicurezza (NTC). Nel quadro di questo progetto, nell'ottobre del 2020 è stato condotto un sondaggio presso i gestori di infrastrutture critiche concernente la necessità di un istituto di test. I risultati sono chiari: circa l'85 per cento delle organizzazioni interpellate ha espresso la necessità di verifiche in ambito di cibersicurezza e la volontà di affidare questi mandati all'NTC. Secondo il 75 per cento dei partecipanti tale fabbisogno continuerà ad aumentare nei prossimi anni e nessuno ritiene che diminuirà.

«Per i prossimi cinque anni, come valuta la necessità di verifiche della cibersicurezza nella Sua organizzazione che affiderebbe a un Istituto Nazionale di Test per la Cibersicurezza?»
N=64



Nel novembre del 2020 è pertanto stata fondata l'associazione NTC. Essa è il motore del progetto e, alla conclusione di quest'ultimo, sarà responsabile dell'esercizio. Finora la Confederazione ha accompagnato l'iniziativa sotto il profilo tecnico. In un intervento parlamentare, nel dicembre del 2020 il consigliere nazionale Franz Grüter ha chiesto la partecipazione della Confederazione alla creazione e all'esercizio dell'NTC (20.4495).
Dal 2021 l'NTC svolge i primi processi di verifica, sviluppa il modello si business e definisce le responsabilità per la messa in esercizio effettiva.

3.2 Marchio di qualità cyber-safe.ch per i Comuni svizzeri

Attualmente la tecnologia dell'informazione svolge un ruolo centrale per i Comuni, dall'esercizio degli impianti di depurazione ai sistemi di riscaldamento comunali fino al Governo elettronico. Pertanto, i Comuni non possono più ignorare la cibersicurezza, a prescindere dalle loro dimensioni e dai mezzi a disposizione. Per questo motivo, da metà 2020 un progetto pilota sostenuto da NCSC, Rete integrata Svizzera per la sicurezza (RSS) e Associazione dei Comuni Svizzeri (ACS) sta testando la cibersicurezza di una quindicina di Comuni svizzeri con l'ausilio del marchio di qualità «cyber-safe.ch», per informarli sulle misure da adottare e, se del caso, conferire il marchio secondo l'esempio dei Comuni di Bussigny (VD) o Jonen (AG). Il progetto pilota dovrebbe permettere all'NCSC di valutare i vantaggi di un marchio di qualità per la cibersicurezza dei Comuni e delle amministrazioni pubbliche e di trarne insegnamenti la definizione di future misure.

3.3 Marchio di qualità per i fornitori di servizi IT

Con l'avanzare della digitalizzazione le piccole e le medie imprese (PMI) sono sempre più esposte alle minacce in agguato nel ciberspazio. Nel contempo le PMI svizzere collaborano sempre di più con fornitori di servizi IT esterni (attualmente due terzi). Poiché questi ultimi influiscono direttamente sulla ciber-resilienza delle PMI, è imperativo che dispongano delle competenze tecniche e organizzative di base in ambito di sicurezza informatica e dell'informazione.
Nell'ultimo trimestre del 2020 un'istituzione pubblica-privata composta da partner della Confederazione e attori dell'economia privata ha lanciato l'iniziativa per la creazione di un marchio di qualità indipendente per fornitori di servizi IT. Il marchio di qualità certifica fornitori di servizi IT che garantiscono ai loro clienti un livello di protezione adeguato adottando le misure tecniche e organizzative necessarie. Il conferimento del marchio di qualità ha quindi un impatto positivo sulla ciber-resilienza delle PMI, garantisce una digitalizzazione di qualità rafforzando in tal modo la fiducia nella sicurezza digitale della Svizzera.
Il concetto del marchio di qualità è stato definito e approntato nel dicembre del 2020. Fra gennaio e marzo 2021 è stato eseguito un progetto pilota con quattro fornitori di servizi IT. Fra maggio e luglio dello stesso anno è stata condotta una fase di test ampliata a 10 fornitori di servizi IT. Parallelamente, nel mese di maggio è stata avviata l'elaborazione di una strategia di pianificazione (strategia «go to market», con sito Internet, comunicazione, misure di marketing, creazione di una rete di ispettori, processo aziendale e operativo). L'entrata sul mercato con il passaggio alla fase di esercizio da parte dell'associazione di nuova costituzione è prevista per il mese di settembre del 2021.

3.4 Campagna nazionale di sensibilizzazione

Dal 3 al 7 maggio 2021 si è svolta la prima settimana di sensibilizzazione alla cibersicurezza. La campagna nazionale è stata patrocinata dall'NCSC, dalla Prevenzione Svizzera della Criminalità (PSC), dalla Scuola universitaria professionale di Lucerna e da Swiss Internet Security Alliance (SISA)/iBarry. Numerosi partner hanno inoltre sostenuto l'ente responsabile promuovendo la campagna sui loro canali. Tra essi figurano digitalswitzerland, Digital Liechtenstein, i membri di SISA (ad es. Swisscom, UPC-Sunrise, SWITCH, La Mobiliare e quasi 100 banche quali interlocutori di «eBanking – ma sicuro!») nonché tutti i corpi di polizia cantonali e comunali.
Per cinque giorni, ogni giorno è stato presentato un tema allo scopo di sensibilizzare i cittadini fornendo loro al contempo ausili per un comportamento responsabile nello spazio digitale. Sono stati trattati i temi: backup dei dati, password, aggiornamenti, protezione antivirus e cautela.

I contenuti sono stati comunicati e diffusi principalmente online, in particolare sui social media.

3.5 Progetto pilota con Bug Bounty Switzerland

L'NCSC ha deciso di avviare un progetto pilota con la società Bug Bounty Switzerland in cui hacker etici sono stati incaricati di individuare eventuali vulnerabilità in alcuni sistemi dell'Amministrazione federale. Per ogni vulnerabilità individuata, gli hacker etici sarebbero stati ricompensati in base alla gravità della falla.
Il progetto pilota è iniziato il 10 maggio 2021 ed è durato 11 giorni. 15 hacker hanno testato in tutto sei sistemi informatici del Dipartimento federale degli affari esteri (DFAE) e dei Servizi del Parlamento (SP) individuando 10 vulnerabilità. Questo numero è relativamente basso per un primo test con un gruppo di hacker etici e mostra che tutti i sistemi verificati dispongono di un alto livello di sicurezza e che non costituiscono un facile bersaglio. Tuttavia, anche in questi ambienti vi sono ancora falle nei sistemi pubblicamente accessibili in Internet nonostante tutte le misure di sicurezza esistenti e provano chiaramente la necessità di un programma bug bounty. Dato il buon esito di questa esperienza, l'NCSC intende continuare a impiegare programmi bug bounty per l'Amministrazione federale.[5]

3.6 Elaborazione di un avamprogetto sull'introduzione dell'obbligo di notifica di ciberattacchi

Nella sua seduta dell'11 dicembre 2020, il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF, nello specifico l'NCSC) di elaborare entro fine 2021, d'intesa con i servizi interessati di tutti i dipartimenti, un avamprogetto sull'introduzione di un obbligo di notifica dei ciberattacchi per i gestori di infrastrutture critiche. A tal fine verrà designato un servizio centrale di notifica incaricato di utilizzare le segnalazioni per migliorare gli allarmi precoci contro i ciberpericoli e di rilevare i dati statistici relativi agli incidenti informatici. Il nuovo obbligo di notifica dovrà essere compatibile con quelli già esistenti (in particolare in ambito di diritto sulla protezione dei dati).
Nel mese di aprile del 2021 l'NCSC ha condotto un sondaggio tra i gestori di infrastrutture critiche in merito all'obbligo di notifica dei ciberattacchi, da cui è emerso un consenso elevato, a condizione che possa essere attuato con un onere amministrativo minimo. La figura 2 mostra il grado di accettazione tra i partecipanti al sondaggio (n=400) su una scala da 1 («Non sono affatto d'accordo con l'introduzione dell'obbligo di notifica») a 5 («Sono pienamente d'accordo con l'introduzione dell'obbligo di notifica»). I risultati del sondaggio serviranno per impostare il progetto da porre in consultazione nel corso del 2021.

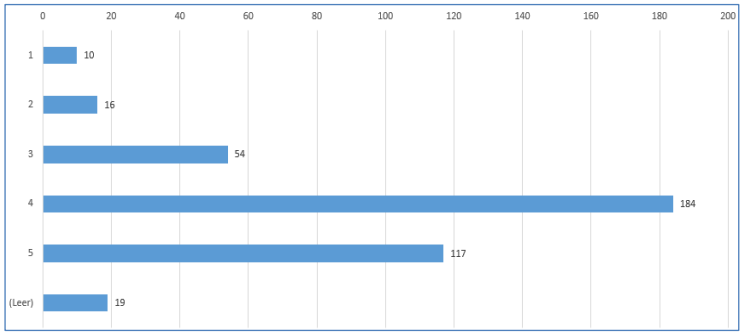


Figura 2: Accettazione dell'obbligo di notifica

[5] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-84304.html

4 Lo stato di attuazione nel dettaglio

Di seguito è presentato lo stato di attuazione della SNPC in relazione alla pianificazione delle tappe fondamentali. Per ogni misura sono raffigurate le tappe fondamentali attuate e quelle non attuate nel secondo trimestre del 2021. Segue una breve descrizione esplicativa.
Su un totale di 275 tappe fondamentali contenute nel piano di attuazione della SNPC, 154 sono state attuate e 8 non sono ancora state attuate. Quindi, 6 misure su 29 sono state completate. Con uno stato di attuazione di quasi due terzi dopo 14 trimestri di SNPC sui 20 totali, si può affermare che l'attuazione della strategia è ancora a buon punto, e quindi i lavori ancora in sospeso potranno essere svolti entro le scadenze previste. La figura 3 mostra lo stato di attuazione di tutte le tappe fondamentali.

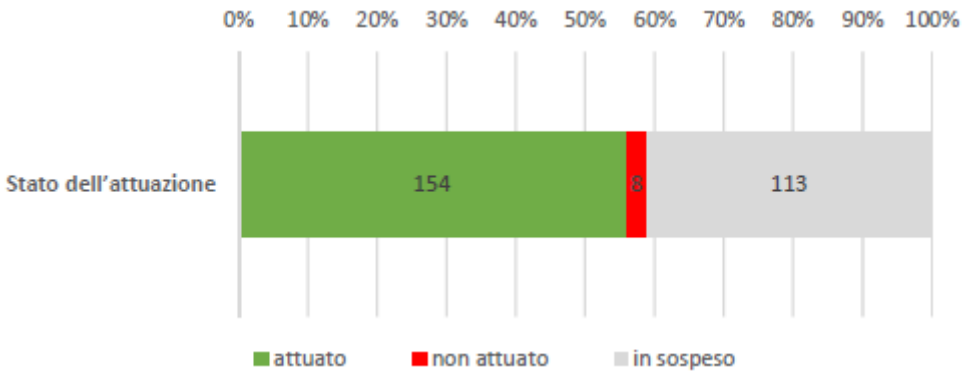


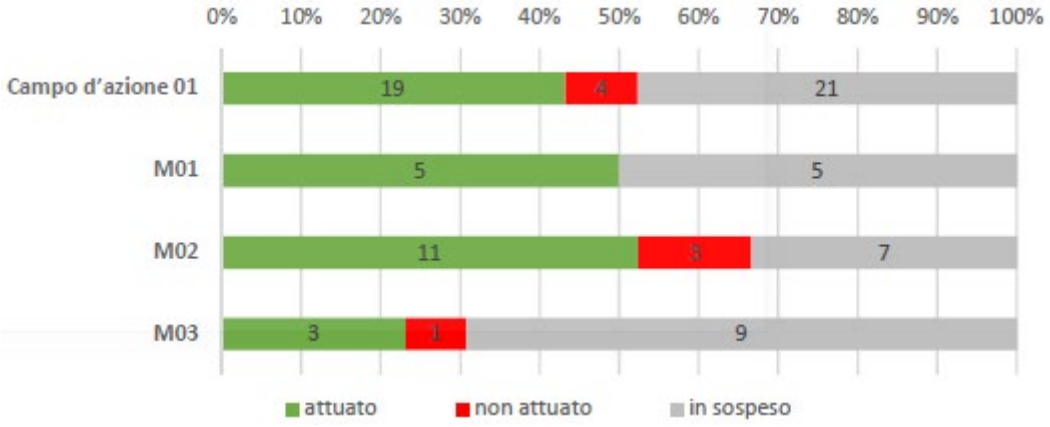
Figura 3: Stato di attuazione delle tappe fondamentali della SNPC

4.1 Campo d'azione 1 "acquisizione di conoscenze e competenze"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M1: Individuazione precoce di tendenze e tecnologie e acquisizione delle conoscenze (armasuisse S+T)
- M2: Ampliamento e promozione delle competenze di ricerca e formazione (NCSC e armasuisse S+T)
- M3: Creazione di condizioni quadro vantaggiose per un'economia della sicurezza delle TIC innovativa in Svizzera (NCSC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

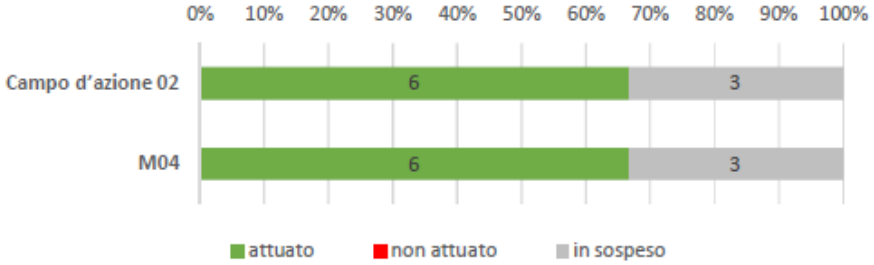
	Tappa fondamentale	Stato
M1	Monitoraggio delle tecnologie: 1) le prestazioni del CYD Campus per il monitoraggio all'attenzione del NCSC sono stabilite 2) avvio del monitoraggio 3) prima valutazione del monitoraggio	Attuata
	Analisi delle tendenze: 1) il piano per il pubblico target e i contenuti sono elaborati, i rapporti sono trasmessi 2) i mandati di valutazione sono conferiti	Attuata
M2	Analisi del fabbisogno per la creazione di offerte formative: 1) prospetto delle offerte di formazione esistenti 2) l'analisi è eseguita e i gruppi target sono definiti	Attuata *«Progetto concluso in anticipo: la panoramica dell'offerta mostra che il mercato è ormai consolidato.»*
	Centro di ricerca e supporto dei due politecnici federali: 1) il piano per il centro di ricerca e supporto è definito 2) gli aspetti riguardanti il finanziamento e l'ubicazione sono chiariti 3) inizio dell'attività del centro di ricerca con graduale potenziamento negli anni 2021–2022	Attuata
	Cyber Defence Campus: 1) il polo di Thun è operativo 2) il polo del PFL è operativo 3) il polo del PFZ è operativo	Attuata
	Promozione della ricerca interdisciplinare e della formazione in materia di cibersicurezza: 1) i principali istituti di ricerca nel settore dei ciber-rischi sono identificati	Attuata
	Promozione dell'«hackeraggio etico»: 1) gli eventi consolidati in materia di hackeraggio etico sono identificati 2) gli strumenti di promozione sono predisposti; domanda di finanziamenti, ove necessari	Attuata Progetto accantonato: *il finanziamento tramite la Confederazione non è il mezzo adatto per promuovere eventi in materia di hackeraggio etico. Fondi investiti nel progetto pilota «Bug bounty».*
	Svolgimento del programma pilota bug bounty: 1) il contratto tra Bug Bounty Switzerland e l'NCSC è stipulato 2) il progetto pilota è realizzato, la valutazione e il rapporto sono disponibili	Attuata
M3	Creazione di centri di innovazione: 1) proposta per la creazione e il finanziamento di un polo nazionale per la cibersicurezza	Progetto accantonato: *a seguito di iniziative esistenti (come «trust valley», «Zuger Initiative» ecc.) e di esperienze tratte da colloqui condotti soprattutto con i Cantoni. Nel Piano di attuazione il progetto viene accantonato e sarà eventualmente rivalutato nel quadro della nuova Strategia SNPC.*
	Think Tank: 1) il piano per il centro di ricerca e supporto di entrambi i politecnici federali è definito 2) gli aspetti riguardanti il finanziamento e l'ubicazione del centro di ricerca e supporto dei due politecnici federali sono chiariti 3) il centro di ricerca con il «think tank» è operativo, con graduale potenziamento negli anni 2021–2022	Attuata

4.2 Campo d'azione 2 "situazione di minaccia"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M4: Rafforzamento delle capacità di valutazione e rappresentazione delle cibermi-nacce (SIC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M4	Identificazione dei gruppi target e delle loro esigenze: 1) identificazione dei gruppi target allargati e delle loro esigenze 2) identificazione dei canali di comunicazione per i diversi gruppi target	Attuata
	Definizione del catalogo di prodotti per ogni gruppo target (catalogo delle prestazioni): 1) l'ambito di competenza della Confederazione e del mondo economico è chiarito 2) catalogo delle prestazioni per ogni gruppo target	Attuata
	Creazione delle fonti e delle risorse produttive necessarie: 1) l'elenco delle ulteriori fonti necessarie è redatto 2) progetto per la creazione del supporto tecnico	Attuata

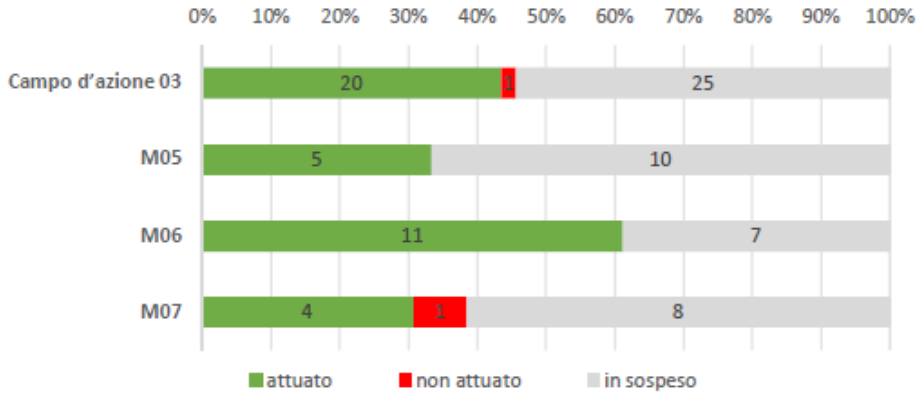
4.3 Campo d'azione 3 "gestione della resilienza"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M5: Miglioramento della resilienza delle TIC delle infrastrutture critiche (UFPP, in collaborazione con gli uffici specializzati in settori sottoposti a regolamentazione)
- M6: Miglioramento della resilienza delle TIC all'interno dell'Amministrazione federale (NCSC)
- M7: Scambio di conoscenze e creazione di basi per migliorare la resilienza delle TIC nei Cantoni (NCSC, RSS)[6]

[6] Per maggiori informazioni su altri progetti concernenti il piano di attuazione dei Cantoni relativo alla SNPC 2018–2022 della RSS e sul rispettivo stato di attuazione si rimanda a: https://www.svs.admin.ch/it/temi/cybersicherheit/cybersicherheit-kantone.html (in tedesco e francese)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M5	Attuazione dei progetti previsti e in corso per rafforzare la resilienza nei sottosettori critici: 1) l'inventario delle disposizioni attuate e di quelle non ancora attuate contemplate dai rapporti sulle misure è redatto 2) le responsabilità per l'attuazione sono chiarite 3) la tabella di marcia / la pianificazione delle misure in atto e imminenti è elaborata	Attuata
	Costituzione del gruppo di lavoro accademico per la cibersicurezza: 1) inventario dei progetti e dei gruppi attivi 2) istituzionalizzazione del gruppo di lavoro	Attuata
M6	Sviluppo di disposizioni in materia di sicurezza per consentire metodi di progetto agili: 1) i compiti attuali e i risultati rilevanti ai fini della sicurezza nei metodi di progetto sono analizzati 2) identificazione e descrizione degli ulteriori compiti e risultati nonché delle aggiunte alle parti esistenti	Attuata
	Campagna di sensibilizzazione nell'Amministrazione federale: 1) il piano di massima della campagna di sensibilizzazione per la sicurezza informatica nell'Amministrazione federale «IKT Security 19» è allestito (T4/2018) 2) la campagna di sensibilizzazione per la sicurezza informatica nell'Amministrazione federale «IKT Security» è avviata 3) la concertazione con altri attori attivi sull'ampliamento concettuale di una campagna di sensibilizzazione nazionale è avvenuta	Attuata
	Trasmissione sicura dei dati (SCION): 1) dichiarazione d'intenti di utenti interessati e partecipanti alla fase pilota 2) creazione e avvio delle applicazioni pilota	Attuata
	Security Operations Center (SOC) UFIT: 1) progetto e piano di attuazione	Attuata
	Creazione di un'interfaccia con il settore dei politecnici federali: 1) coordinamento con il delegato alla cibersicurezza 2) messa in atto di misure concrete 3) coordinamento congiunto	Attuata
M7	Scambi permanenti tra Cantoni e Centro di competenza per la cibersicurezza: 1) accertamento dei requisiti della dotazione del posto di lavoro presso l'NCSC	Progetto accantonato: *il progetto è stato sospeso in primo luogo a causa della pandemia e sarà rivalutato all'inizio del 2022 in considerazione dell'orientamento dell'NCSC.*

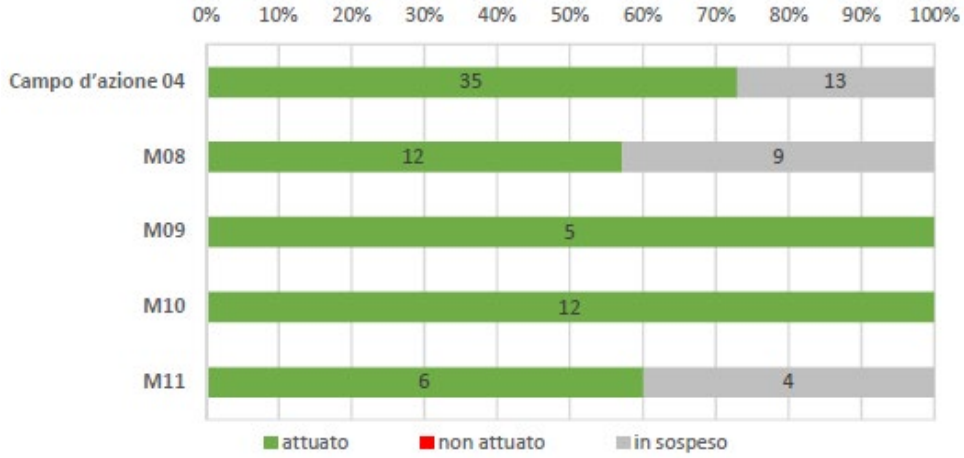
	Svolgimento della «Ciber-Landsgemeinde»: 1) svolgimento della «Ciber-Landsgemeinde» 2019 2) svolgimento della «Ciber-Landsgemeinde» 2020	Attuata
	Interfaccia tra PFZ e Cantoni: 1) coordinamento con la RSS 2) messa in atto di misure concrete	Attuata

4.4 Campo d'azione 4 "standardizzazione / regolazione"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M8: Sviluppo e introduzione di standard minimi (UFAE)
- M9: Verifica dell'obbligo di notifica dei ciberincidenti e decisione in merito alla relativa introduzione
- M10: Internet governance globale (UFCOM)
- M11: Acquisizione di know-how su aspetti della standardizzazione collegati alla sicurezza informatica (NCSC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M8	Sviluppo e attuazione di standard minimi per migliorare la resilienza delle TIC: 1) pubblicazione dello standard minimo TIC e strumenti per l'assessment 2) standard minimo secondo il manuale per la protezione di base «Handbuch Grundschutz» (in tedesco e francese) dell'Associazione delle aziende elettriche svizzere 3) standard dei settori approvvigionamento idrico, derrate alimentari, gas naturale e trasporti pubblici	Attuata
	Sviluppo e approntamento di ausili per le PMI: 1) pubblicazione del test di cibersicurezza online per le PMI (SATW) nel terzo trimestre del 2018 2) analisi del fabbisogno di altri strumenti (ausili tecnici, marchi di qualità, guide, istruzioni) per le PMI 3) conclusione della verifica della possibile introduzione di marchi di qualità e norme	Attuata
	Marchio di qualità Cyber Safe per Comuni: 1) il contratto tra Cyber-Safe e l'NCSC come pure l'accordo tra l'NCSC e l'Associazione dei Comuni Svizzeri sono firmati 2) la tabella di marcia del progetto è definita e gli accordi con i 15 Comuni pilota sono stipulati	Attuata
	Marchio di qualità per i fornitori di servizi IT: 1) il contratto tra Digitalswitzerland e l'NCSC è firmato	Attuata

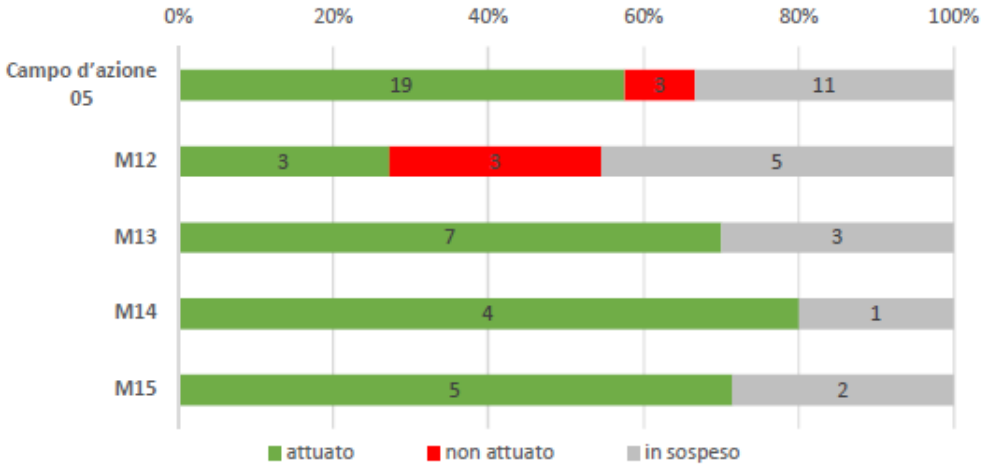
	2) elaborazione delle basi per il marchio di qualità (manuale di verifica, lista di controllo ecc.)	
M9	Studio dei modelli di massima degli obblighi di notifica: 1) messa a concorso ed elaborazione di uno studio di base 2) rapporto sui modelli di massima e raccomandazioni in materia	Attuata
	Dibattito di principio con il mondo economico e le autorità: 1) prosieguo del dibattito con i rappresentanti della politica e dell'economia 2) base per la decisione di introdurre l'obbligo di notifica	Attuata
M10	Incontro del gruppo di alto livello istituito dal Segretario generale delle Nazioni Unite: 1) incontro a New York, Ginevra e Helsinki 2) rapporto finale del progetto 3) valutazione delle possibilità di attuazione del rapporto	Attuata
	Piattaforme di scambio multistakeholder per il coordinamento a livello nazionale: 1) Swiss-IGF 2018 (T4/2018) 2) Swiss-IGF 2020	Attuata
M11	Creazione di un pool di esperti interdipartimentale in materia di cibersicurezza: 1) accertamento del fabbisogno 2) ideazione del pool di esperti e deliberazione delle risorse	Attuata
	Rafforzamento dei progetti di standardizzazione con il supporto delle Scuole universitarie: 1) il progetto del centro comune di ricerca e supporto PFL-PFZ è elaborato 2) panoramica delle attività condotte in Svizzera in questo ambito 3) attuazione delle attività nei gruppi di lavoro identificati come strategici	Attuata
	Contributo della Svizzera ad ancorare il tema della cibersicurezza nella politica finanziaria internazionale: 1) primo rapporto intermedio sulle attività di rafforzamento delle capacità internazionali in ambito di cibersicurezza nel settore finanziario	Attuata

4.5 Campo d'azione 5 "Gestione degli incidenti"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M12: Potenziamento di MELANI come partenariato pubblico-privato per i gestori di infrastrutture critiche (NCSC)
- M13: Creazione di servizi per tutte le imprese (NCSC)
- M14: Collaborazione della Confederazione con gli uffici competenti e i centri di competenze (NCSC)
- M15: Processi e basi della gestione degli incidenti nell'Amministrazione federale (NCSC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M12	Ampliamento mirato della cerchia chiusa di clienti: 1) l'analisi della situazione in merito all'utilizzo di MELANI da parte dei diversi settori critici è effettuata	Rimandato: *sulla base dello sviluppo strategico, vi saranno una rivalutazione e una nuova pianificazione all'inizio del 2022*
	Sviluppo e ampliamento della gamma di servizi e prodotti: 1) analisi della gamma di prodotti e servizi di MELANI e dell'attuale fabbisogno	Attuata
	Potenziamento dell'attuale piattaforma di scambio: 1) lo studio con le varianti raccomandate di MELANI-NET 2.0 è redatto (T3/2018) 2) la prova di fattibilità in merito alla variante raccomandata è effettuata 3) piano MELANI-NET 2.0 4) e MELANI-NET 2.0 è operativo	Attuata Attuata Rimandato: *a seguito dello sviluppo strategico delle piattaforme d'informazione dell'NCSC, vi saranno una rivalutazione e una nuova pianificazione all'inizio del 2022*
M13	Istituzione di un servizio nazionale di contatto ciber: 1) il piano di massima del portale online per la segnalazione di incidenti informatici è allestito 2) il portale online per le segnalazioni di incidenti informatici è a disposizione del pubblico 3) integrazione nella piattaforma d'informazione sui ciber-rischi (cfr. M29)	Attuata
	Informazione tempestiva mediante l'app Alertswiss in caso di incidente: 1) accertamento delle esigenze di allarme, allerta e informazione del pubblico in caso di incidente informatico tra il Centro di competenza e l'UFPP 2) il piano di integrazione delle ciberinformazioni nella app Alertswiss è allestito 3) possibilità di informare il pubblico in caso di ciberevento mediante l'app Alertswiss 4) pubblicazione dell'informazione concernente la novità (ciberevento) nell'app Alertswiss	Attuata
M14	Panoramica dei SOC e dei CERT attualmente operativi con i rispettivi interlocutori: 1) il censimento dei SOC e dei CERT attualmente operativi, inclusi i rispettivi interlocutori, è realizzato e documentato 2) definizione del processo e delle responsabilità riguardanti l'aggiornamento corrente della panoramica	Attuata
	Scambio di informazioni con i CERT e i SOC: 1) analisi del fabbisogno e delle possibilità di uno scambio sistematico di informazioni 2) definizione e attribuzione dei progetti per la messa in atto dello scambio di informazioni	Attuata
M15	Elaborazione di un'ordinanza in materia di cibersicureza: 1) elaborazione dell'ordinanza 2) approvazione dell'ordinanza da parte del Consiglio federale 3) l'entrata in vigore dell'ordinanza è fissata	Attuata
	Predisposizione di un processo di gestione degli incidenti informatici per l'Amministrazione federale:	

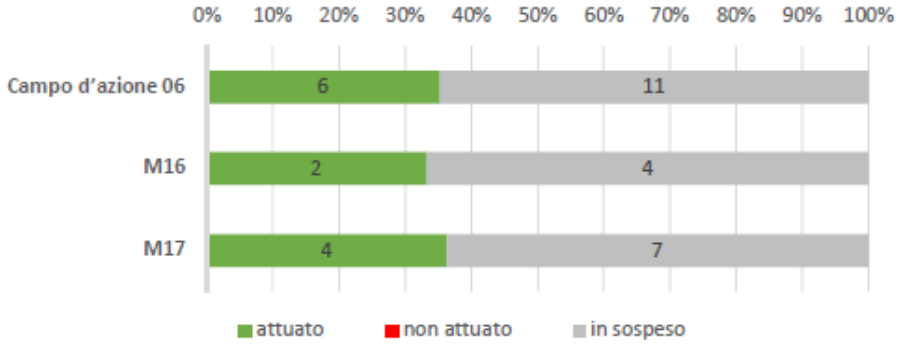
	1) prima bozza di un processo, discussione con i fornitori di prestazioni e i servizi coinvolti (T3/2018) 2) adeguamento del processo all'ordinanza in materia di cibersicurezza	Attuata

4.6 Campo d'azione 6 "Gestione delle crisi"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M16: Integrazione dei servizi deputati alla cibersicurezza negli stati maggiori di crisi della Confederazione (NCSC)
- M17: Esercizi congiunti di gestione delle crisi (NCSC, Segreteria generale del DDPS)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

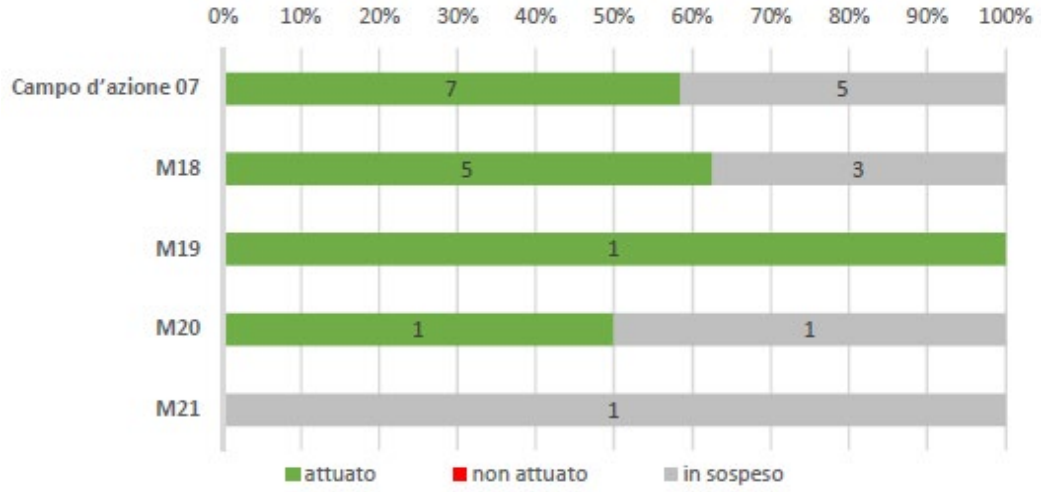
	Tappa fondamentale	Stato
M16	Arricchimento del lessico del ciberspazio: 1) inventario delle definizioni esistenti 2) revisione/elaborazione del glossario del ciberspazio	Attuata
M17	Creazione delle basi per le esercitazioni di crisi che implicano aspetti inerenti al ciberspazio: 1) inventario delle esercitazioni di crisi nazionali e internazionali in essere e previste che implicano aspetti inerenti al ciberspazio 2) processo per aggiornare e coordinare con la panoramica delle cibere esercitazioni	Attuata
	Svolgimento di esercizi specifici di settore: 1) l'analisi del fabbisogno di esercitazioni in caso di crisi in settori specifici è effettuata	Attuata
	Introduzione di aspetti inerenti al ciberspazio nelle esercitazioni di crisi trasversali: 1) concertazione con i partner responsabili sull'inclusione nell'esercizio di criteri pertinenti al ciberspazio	Attuata

4.7 Campo d'azione 7 "Perseguimento penale"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M18: Panoramica dei casi in materia di criminalità informatica (fedpol, CCPCS con NEDIK)
- M19: Rete di supporto alle indagini nella lotta alla criminalità digitale (fedpol come componente della CCPCS)
- M20: Formazione (CCPCS incl. fedpol, RSS incl. Ministero pubblico della Confederazione)
- M21: Ufficio centrale per la criminalità informatica (fedpol)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

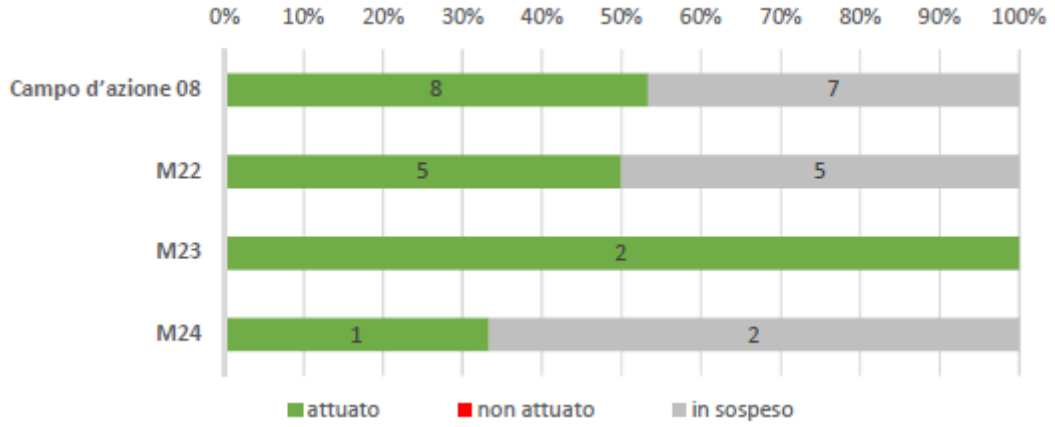
	Tappa fondamentale	Stato
M18	Casistica della criminalità informatica (PICSEL): 1) avvio della fase di test PICSEL	Attuata
	Elaborazione di una casistica giudiziaria: 1) software Cyber-CASE; elenco della serie di casi di tutti gli SPOC ciber dei Ministeri pubblici (già operativo) 2) software online per la panoramica dei procedimenti in corso	Attuata
	Presentazione degli sviluppi, degli scenari e delle ripercussioni della criminalità informatica: 1) bollettino mensile (della polizia) NEDIK 2) panoramica dei procedimenti in corso (della polizia & giudiziari)	Attuata
M19	Basi giuridiche concernenti la collaborazione e il computo delle prestazioni tra Confederazione e Cantoni nonché tra Cantoni: 1) accordo(i) firmato(i) e approvato(i)	Attuata
M20	Attuazione dei piani di formazione: 1) panoramica delle possibilità di formazione a livello accademico (della polizia)	Attuata
M21	Nessuna tappa fondamentale entro il secondo trimestre del 2021	

4.8 Campo d'azione 8 "Ciberdifesa"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M22: Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici (SIC)
- M23: Capacità di attuazione di misure attive nel ciberspazio secondo la LAIn e la LM (SIC, BAC-CEO)
- M24: Garanzia della prontezza operativa dell'esercito nel ciberspazio in ogni circostanza e regolamentazione del suo ruolo sussidiario di supporto delle autorità civili (Segreteria generale del DDPS, BAC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

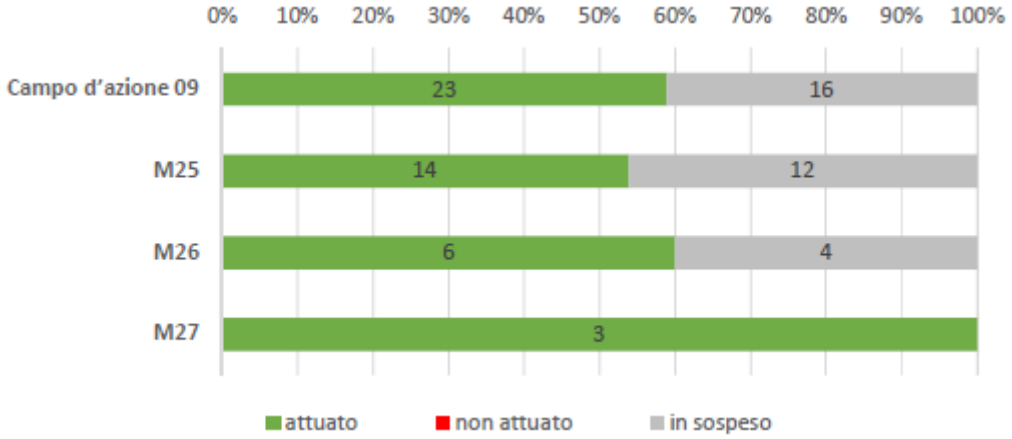
	Tappa fondamentale	Stato
M22	Capacità di acquisizione delle informazioni e di attribuzione: 1) la prima tappa dell'ampliamento è realizzata	Attuata
	Svolgimento di una formazione specifica in ciberdifesa (Esercito): 1) prima esercitazione con la BAC delle Forze terrestri 2) avvio del corso di master congiunto PFL-PFZ-DDPS 3) primi corsi organizzati dal PFL e dal DDPS 4) introduzione del curriculum «Ciberdifesa» («Cyber Defence»)	Attuata
M23	Utilizzo delle capacità del COE-BAC sviluppate nel quadro della LAIn: 1) discussione con gli uffici specializzati sugli effetti collaterali indesiderati delle attività previste 2) le capacità sono disponibili	Attuata
M24	Conclusione del progetto per lo sviluppo della ciberdifesa	Attuata

4.9 Campo d'azione 9 "Posizionamento attivo della Svizzera nella politica di sicurezza informatica internazionale"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M25: Ruolo attivo nella definizione e partecipazione ai processi di politica in materia di sicurezza esterna in ambito informatico (DFAE, SECO)
- M26: Cooperazione internazionale per la crescita e lo sviluppo delle capacità nel settore della sicurezza informatica (DFAE)
- M27: Consultazioni politiche bilaterali e dialoghi multilaterali sulla politica in materia di sicurezza esterna in ambito informatico (DFAE)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M25	Partecipazione ai processi dell'ONU: 1) rapporti annuali 2019 e 2020	Attuata
	Rappresentanza degli interessi nell'ambito dell'OSCE (consolidamento del clima di fiducia tra gli Stati): 1) adesione ai negoziati, partecipazione attiva al processo e rapporti annuali 2019 e 2020	Attuata
	Creazione e istituzione dell'iniziativa «Geneva Dialogue on responsible behavior in Cyberspace»: 1) piano per l'istituzione del Geneva Dialogue come piattaforma multistakeholder 2) 2–3 tornate di dialogo del processo di esperti in merito all'applicazione del diritto internazionale pubblico nel ciberspazio hanno avuto luogo 3) integrazione nell'UNGGE e nell'OEWG degli elementi acquisiti nel processo di esperti 4) integrazione nei rapporti conclusivi dell'UNGGE e dell'OEWG degli interessi della Svizzera nell'applicazione del diritto internazionale pubblico al ciberspazio	Attuata
	Osservazione degli sviluppi in seno all'Unione europea (in particolare del Servizio europeo per l'azione esterna e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, ENISA): 1) l'analisi dei principali attori, dei processi e delle misure dell'UE è effettuata; all'interno di essa sono stati identificati i servizi coinvolti in Svizzera 2) analisi delle possibili ripercussioni delle diverse misure adottate dall'UE per la Svizzera	Attuata

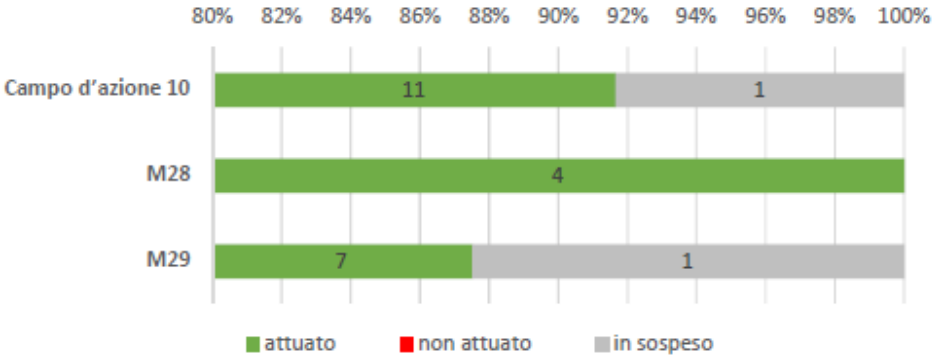
	Impegno volto a promuovere un ciberspazio aperto e libero: 1) quadro dei processi riguardanti i diritti dell'uomo e dei forum rilevanti 2) valutazione della partecipazione della Svizzera a processi e forum scelti	Attuata
M26	Organizzazione di workshop con organizzazioni regionali: 1) preparazione del piano e svolgimento del primo workshop a Ginevra	Attuata
	Organizzazione di workshop per la creazione di istituzioni e strutture in materia di cibersicurezza esterna: 1) analisi del fabbisogno, esercitazioni, piano, svolgimento del primo workshop	Attuata
M27	Sino-European Cyber Dialogue (SECD): 1) costituzione del gruppo di lavoro «International Law» 2) continuazione dei lavori	Attuata
	MENA Cybersecurity Forum: 1) proseguimento del MENA Cybersecurity Forum	Attuata

4.10 Campo d'azione 10 "Visibilità e sensibilizzazione"

Panoramica del campo d'azione: misure e responsabilità di attuazione

- M28: Creazione e attuazione di un piano per la comunicazione di informazioni sulla SNPC (NCSC)
- M29: Sensibilizzazione del pubblico sui rischi informatici (NCSC)

Stato di attuazione



Tappe fondamentali dal 2018 al 2° trimestre 2021

	Tappa fondamentale	Stato
M28	Elaborazione di un piano per la comunicazione di informazioni sulla SNPC: 1) l'analisi della situazione è effettuata 2) piano per la comunicazione di informazioni sulla SNPC (obiettivi, gruppi target, messaggi, attuazione degli obiettivi [strategia], strumenti/misure, quantificazione dei successi ottenuti e bilancio preventivo) 3) definizione delle responsabilità della comunicazione e dei relativi termini (programma) d'intesa con altri attori della SNPC 4) avvio dell'attuazione del piano per la comunicazione	Attuata
M29	Sviluppo e svolgimento di una campagna nazionale di sensibilizzazione: 1) la concertazione con altri attori attivi sull'elaborazione concettuale di una campagna di sensibilizzazione nazionale è avvenuta 2) il piano per la campagna nazionale è definito 3) piano di attuazione 4) avvio/produzione della campagna nazionale	Attuata

	Piattaforma d'informazione sui ciber-rischi: 1) sviluppo del progetto della piattaforma (contenuti) 2) lancio della piattaforma sulla campagna di sensibilizzazione 3) valutazione dell'utilizzo della piattaforma e adeguamento dei contenuti	Attuata