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

Stato primo trimestre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

Indice

1 Premessa

Un anno fa ho assunto la funzione di delegato federale alla cibersicurezza. Da allora ho imparato molto sulle competenze e sui processi in seno alla Confederazione. Ho incontrato donne e uomini motivati che lavorano insieme in modo costruttivo, trasversalmente alle strutture organizzative. La collaborazione e lo scambio, sia all'interno che all'esterno dell'Amministrazione federale, sono in effetti fondamentali. Lo sono soprattutto per l'attuazione coordinata della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022. Tale strategia fissa gli obiettivi in materia di protezione contro i ciber-rischi in tutti i campi d'azione. La sua attuazione è sostenuta in gran parte da rappresentanti dei Cantoni, dell'economia, delle università e della società. Questa collaborazione funziona bene, lo dimostrano l'avanzamento dei lavori relativi alla SNPC e le misure per migliorare il coordinamento degli attori.

Dall'adozione della SNPC 2018–2022, il Consiglio federale ha definito e attuato la nuova organizzazione della Confederazione nell'ambito dei ciber-rischi. In vigore dal 1° luglio 2020, l'ordinanza sui ciber-rischi costituisce la base giuridica e disciplina la collaborazione in seno all'Amministrazione federale e con i Cantoni, l'economia e la scienza. Il Centro nazionale per la cibersicurezza è operativo. Il Comitato ristretto Ciber e il Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi sono gli organi interdipartimentali che consentono di garantire lo stretto coordinamento di tutti gli attori.

Nei vari campi d'azione della SNPC si riscontrano notevoli progressi. Per quanto riguarda la promozione della ricerca e della formazione, sono state raggiunte tappe importanti come l'introduzione del nuovo esame di professione per futuri Cyber Security Specialist e l'apertura del Cyber Defense Campus presso i due politecnici federali e a Thun. Le piccole e medie imprese (PMI) beneficiano di un sostegno sempre maggiore nella protezione contro i ciber-rischi. Al proposito va menzionato il nuovo marchio di qualità cyber-safe.ch, che permette alle PMI di documentare in maniera trasparente e uniforme il proprio livello di cibersicurezza. Il coordinamento della lotta alla cibercriminalità è stato migliorato grazie all'istituzione del Cyberboard, che riunisce i principali attori del perseguimento penale. Inoltre, la ciberdiplomazia assume una rilevanza sempre maggiore nella politica estera digitale della Svizzera. Di recente, infatti, è stato aperto un dialogo con gli Stati Uniti e prosegue il Geneva Dialogue on Responsible Behaviour in Cyberspace.

Siamo a buon punto. Tuttavia, lo stato di attuazione della SNPC mostra che c'è ancora molto da fare. Constato ad esempio che l'Amministrazione federale deve recuperare il ritardo nel settore della protezione di base così come nella sensibilizzazione e nella formazione continua dei collaboratori. Ritengo altresì che i risultati conseguiti nel settore ciber debbano poter essere valutati oggettivamente. Vogliamo che siano misurabili e che permettano di formulare critiche più puntuali. Dobbiamo perciò definire criteri di misurazione chiari e poi applicarli in modo uniforme. È inoltre imminente una decisione di principio: il Consiglio federale intende pronunciarsi, entro la fine del 2020, sull'introduzione di un obbligo di notifica dei ciberincidenti.
La cibersicurezza è e rimane un processo e noi lo seguiamo passo passo. Sono convinto che più la collaborazione fra tutti gli attori è efficace, più la Svizzera sarà protetta contro i ciber-rischi.

Florian Schütz

2 Stato di attuazione: quadro generale

Il piano di attuazione della SNPC definisce 247 tappe fondamentali, articolate in 29 misure. Nel primo trimestre del 2020, 72 tappe fondamentali sono state attuate, 23 sono state rimandate e 3 non sono state attuate. 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.

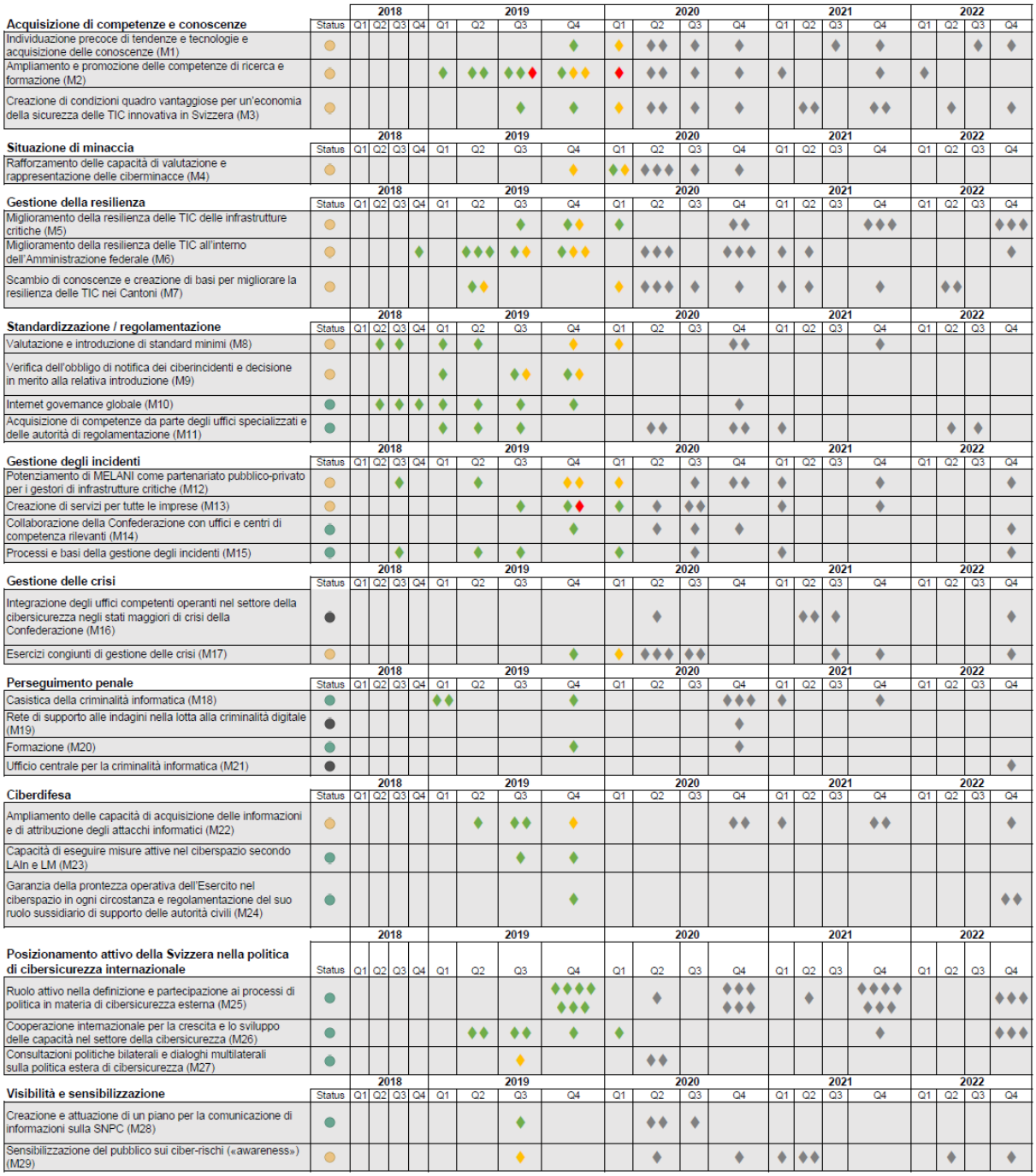


Figura 1: Panoramica dello stato di attuazione

3 Stato: organizzazione in vista dell'attuazione

Negli ultimi due anni, il settore dei ciber-rischi della Confederazione è stato gradualmente riorganizzato. Di seguito le pertinenti decisioni del Consiglio federale e lo stato di attuazione in riferimento alle decisioni prese.

3.1 Panoramica delle decisioni del Consiglio federale

Dopo aver approvato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022 ad aprile 2018, il Consiglio federale ha adottato altre decisioni riguardanti l'attuazione della strategia e l'organizzazione della Confederazione in materia di ciber-rischi. La figura 2 ne presenta una sintesi.

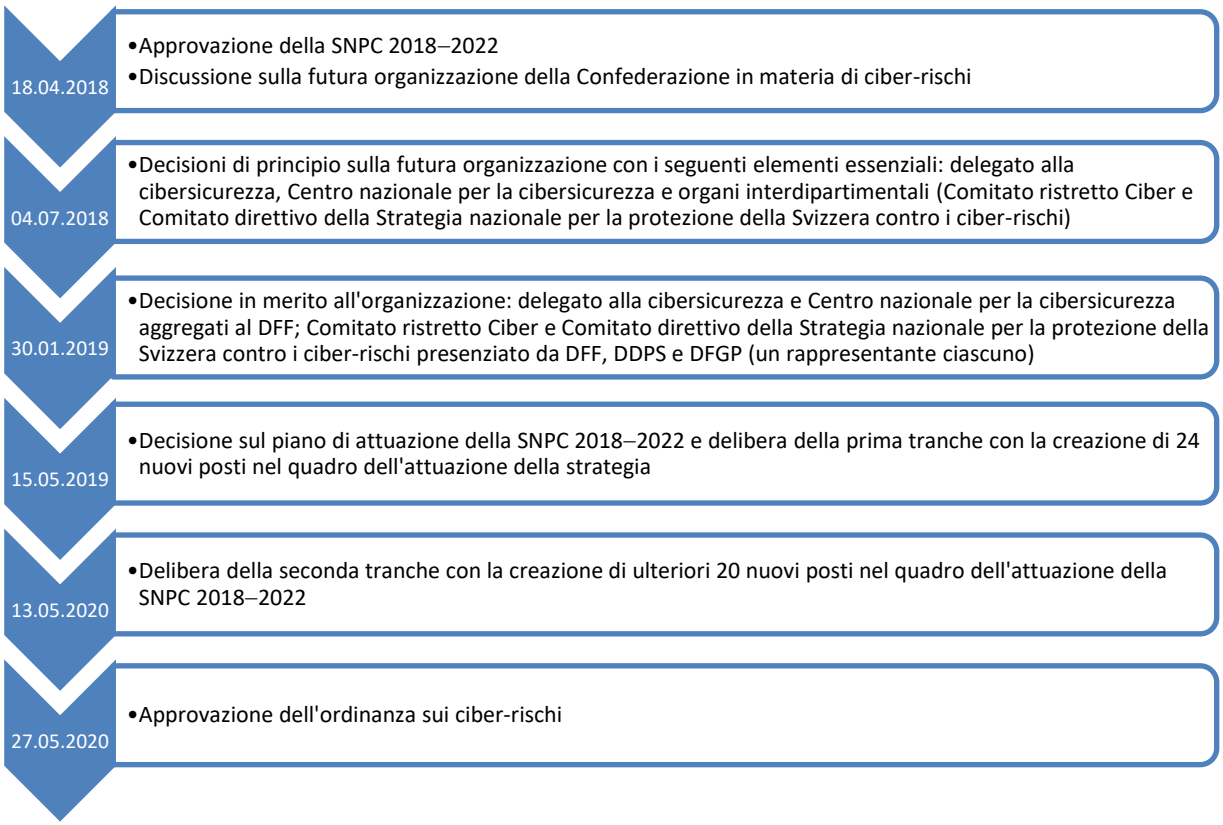


Figura 2: Panoramica delle decisioni del Consiglio federale

Oltre alle decisioni summenzionate, il Consiglio federale ha licenziato i seguenti rapporti in adempimento a diversi postulati depositati, attinenti alle tematiche della cibersicurezza:

- 27.11.2019: rapporto relativo all'organizzazione della Confederazione per l'attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi, in adempimento del postulato Golay 16.4073 del 15.12.2016 e del postulato CPS-N 18.3003 del 22.01.2018 nonché della mozione Eder 17.3508 del 15.6.2017;
- 13.12.2019: rapporto sulle varianti per l'attuazione di un obbligo di notifica in caso di gravi incidenti legati alla sicurezza delle infrastrutture critiche, in adempimento del postulato Graf-Litscher 17.3475 del 15.06.2017;
- 29.04.2020: rapporto sullo standard di sicurezza per i dispositivi connessi a Internet («Internet of Things», IoT), in adempimento del postulato Glättli 17.4295 del 15.12.2017 e del postulato Reynard 19.3199 del 21.03.2019.

3.2 Stato di attuazione degli organi interdipartimentali e del Centro nazionale per la cibersicurezza

L'organizzazione della Confederazione nell'ambito dei ciber-rischi comprende, quali elementi cardine, tre organi interdipartimentali (il Comitato per la cibersicurezza del Consiglio federale, il Comitato ristretto Ciber e il Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi), il delegato alla cibersicurezza quale interlocutore principale della Confederazione e il Centro nazionale per la cibersicurezza (NCSC) quale centro di competenza della Confederazione in materia di ciber-rischi.
Il presente numero illustra le attività degli organi interdipartimentali e del delegato alla cibersicurezza e presenta una descrizione dello stato dei lavori nella creazione del NCSC.

Figura 3: Organizzazione della Confederazione nell'ambito dei ciber-rischi

3.2.1 Comitato per la cibersicurezza del Consiglio federale

Nel primo semestre del 2020, il Comitato per la cibersicurezza del Consiglio federale si è riunito tre volte. Alle riunioni, presiedute dal capo del Dipartimento federale delle finanze (DFF), hanno partecipato i capi del Dipartimento federale di giustizia e polizia (DFGP) e del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), il presidente della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) e il delegato federale alla cibersicurezza. Il comitato riceve informazioni aggiornate sulla situazione di minaccia, discute affari del Consiglio federale rilevanti per la cibersicurezza e tratta questioni politico-strategiche.

3.2.2 Delegato federale alla cibersicurezza

Florian Schütz[1] ha assunto la funzione di delegato federale alla cibersicurezza nell'agosto del 2019. È direttamente subordinato al capo del DFF e coordina gli organi interdipartimentali

[1] Florian Schütz ha un master in scienze informatiche e un Master of Advanced Studies in politica di sicurezza e

per migliorare la collaborazione dei lavori nell'ambito dei ciber-rischi. Inoltre dirige il neocostituito NCSC che, quale centro di competenza della Confederazione, è il primo punto di contatto per l'economia, l'amministrazione, gli istituti di formazione e la popolazione per le questioni in materia di ciber-rischi.

3.2.3 Comitato ristretto Ciber

Analogamente al Comitato per la cibersicurezza del Consiglio federale, il Comitato ristretto Ciber si compone di un rappresentante del DFF (Segreteria generale), di un rappresentante del DFGP (Ufficio federale di polizia), di un rappresentante del DDPS (Segreteria generale) e del presidente della Conferenza dei Comandanti delle Polizie Cantonali della Svizzera (CCPCS). Il Comitato ristretto Ciber, che nel 2019 si è riunito nove volte, è presieduto dal delegato federale alla cibersicurezza. Il Comitato ristretto Ciber prepara le riunioni del Comitato per la cibersicurezza del Consiglio federale e provvede altresì a garantire la migliore collaborazione possibile nell'ambito dei ciber-rischi. Per assolvere ai compiti di coordinamento e includere nel Comitato ristretto Ciber altri importanti attori che si occupano di diverse tematiche ciber, si è deciso di estendere questo comitato quando l'ordine del giorno delle riunioni non riguarda direttamente la preparazione delle riunioni del Comitato per la cibersicurezza del Consiglio federale. Al comitato esteso partecipa il Dipartimento federale degli affari esteri (DFAE) quale rappresentante permanente, segnatamente l'Ufficio dell'Inviato speciale per la politica estera e di sicurezza in ambito cyber. Il delegato federale alla cibersicurezza invita all'occorrenza altri attori.

3.2.4 Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi

Il Comitato direttivo della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (CD SNPC) assicura la coerenza strategica nell'attuazione delle misure della SNPC, coordina gli attori coinvolti ed esamina costantemente l'avanzamento mediante un controlling strategico. Il CD SNPC si è riunito per la prima volta nel novembre del 2019. Vi sono rappresentate le organizzazioni direttamente responsabili dell'attuazione delle misure della SNPC. Nello specifico si tratta delle organizzazioni elencate di seguito.

- Unità amministrative della Confederazione: NCSC, Scienza + Tecnologia di armasuisse (armasuisse S+T), Ufficio federale della protezione della popolazione (UFPP), Ufficio federale delle comunicazioni (UFCOM), Cancelleria federale (CaF), Ufficio federale per l'approvvigionamento economico del Paese (UFAE), Ufficio dell'Inviato speciale per la politica estera e di sicurezza in ambito cyber del DFAE, Ufficio federale di polizia (fedpol), Segreteria generale del Dipartimento federale dell'interno (DFI), Segreteria generale del DDPS, Servizio delle attività informative della Confederazione (SIC), Base d'aiuto alla condotta dell'esercito (BAC).
- Cantoni: CDDGP, Rete integrata Svizzera per la sicurezza (RSS), Cyberboard.
- Economia: ICTswitzerland, SWITCH, Swiss Cyber Experts, Association suisse pour le label de cybersécurité.
- Università: Politecnico federale di Zurigo (PFZ), Politecnico federale di Losanna (PFL).

gestione delle crisi conseguiti al Politecnico federale di Zurigo. Possiede oltre 10 anni di esperienza dirigenziale nel settore della sicurezza informatica nell'economia privata.

3.2.5 Centro nazionale per la ciberiscurezza

Il NCSC è un'unità indipendente della Segreteria generale del DFF dall'agosto del 2019. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI è stata integrata nel centro e ne costituisce il nucleo. Nel 2019 il NCSC è stato riorganizzato ed esteso. In particolare:

- è stato istituito il Servizio nazionale di contatto per le segnalazioni di incidenti e le questioni inerenti ai ciber-rischi, operativo dal 1° gennaio 2020. Questo servizio, che riceve in media 200 segnalazioni alla settimana, esegue una prima analisi delle segnalazioni, inoltrandole poi se necessario ai servizi competenti;

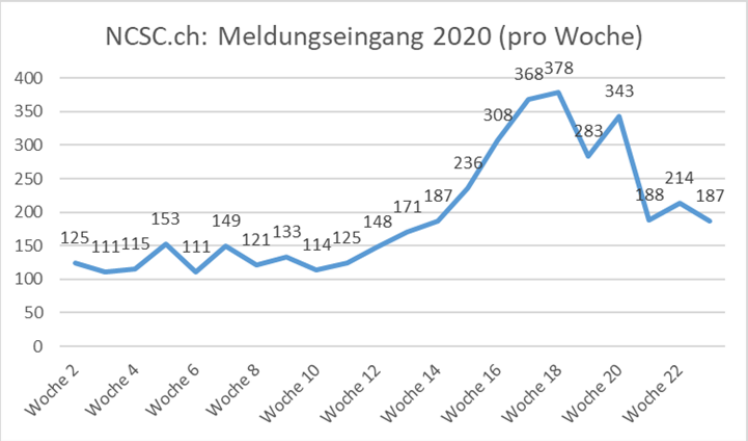


Figura 4: Numero di segnalazioni alla settimana (stato maggio 2020)

- è stato potenziato l'organico del Computer Emergency Response Team (GovCERT) quale servizio specializzato nazionale;
- è stata ampliata la Segreteria del NCSC.

Dal 2020 all'interno del NCSC sarà istituito un pool di esperti che supporterà gli uffici specializzati nei progetti del settore ciber e rafforzerà l'ambito relativo alla sensibilizzazione dell'opinione pubblica.

4 Priorità nell'attuazione della SNPC

Parallelamente alla nuova organizzazione della Confederazione proseguono i lavori di attuazione della SNPC. Questa strategia non è portata avanti solo dall'Amministrazione federale, bensì sostenuta in modo significativo dai Cantoni, dall'economia, dalle università e più in generale dalla società. Mentre al numero 5 si delineano le tappe fondamentali attuate nei singoli campi d'azione, il numero 4 è incentrato sui progetti chiave dei lavori in corso.

4.1 Supporto alle piccole e medie imprese nella protezione dai ciber-rischi

Le piccole e medie imprese (PMI) non facevano parte del gruppo target della prima SNPC 2012–2017. Di conseguenza, finora sono ancora poche le misure coordinate su scala nazionale a supporto delle PMI. Per migliorare la situazione, con l'attuazione della SNPC 2018-2022 saranno avviati progetti in diversi campi d'azione.

4.1.1 Test rapido per PMI, guida e toolkit per la cibersicurezza

In occasione di un'iniziativa[2] ampiamente sostenuta, nel 2018 è stato approntato un test rapido di cibersicurezza per le PMI. L'iniziativa si proponeva di offrire uno strumento di autovalutazione alle PMI, in particolare alle imprese più piccole. Il test rapido[3] consente anche a imprese che non possiedono competenze avanzate nei settori dell'informatica e della sicurezza informatica di accertare in modo semplice e veloce se le misure di protezione dai ciber-rischi di carattere tecnico, organizzativo e del personale sono sufficienti.
In occasione della pubblicazione del test, le PMI hanno espresso l'esigenza di ottenere istruzioni concrete per migliorare la propria cibersicurezza. Per questo motivo, ICTswitzerland e l'Accademia svizzera delle scienze tecniche (SATW) hanno redatto, sempre con la collaborazione di specialisti della Confederazione e dell'economia, un manuale[4] finalizzato a garantire alle PMI almeno una protezione di base. Inoltre, con la Global Cyber Alliance (GCA) è stata conclusa una convenzione per fare in modo che i contenuti (toolkit gratuiti e manuale)[5] siano tradotti e resi disponibili alle PMI svizzere.

Figura 5: Global Cyber Alliance (GCA)

[2] L'iniziativa è appoggiata da: ICTswitzerland, Information Security Society Switzerland (ISS), SATW, Schweizerische Normen-Vereinigung (SNV), Associazione svizzera per sistemi di qualità e di gestione (SQS), Associazione Svizzera d'Assicurazioni (ASA) e rappresentanti della Confederazione.

[3] www.cibersecurity-check.ch (in tedesco, francese e inglese)

[4] https://ictswitzerland.ch/content/uploads/2020/03/Leitfaden_Cybersecurity_Schnelltest_D.pdf (in tedesco)

[5] https://gcatoolkit.org/de/kmu/ (in tedesco, francese, inglese e spagnolo)

4.1.2 Marchio di qualità Cyber Safe

Standard mancanti o troppo complicati impediscono alle PMI di valutare in modo trasparente il proprio livello nel settore della cibersicurezza e di documentarlo anche nei confronti di terzi. Il marchio di qualità Cyber Safe, concepito dall'Association Suisse pour le Label de Cybersécurité, consente di ovviare a questo problema. Il marchio è frutto di un'iniziativa privata e il percorso di certificazione è stato elaborato in stretta collaborazione con un gruppo di rappresentanti delle PMI[6]. Lanciato il 18 dicembre 2019, il marchio contribuisce in modo significativo all'attuazione della SNPC. Maggiori informazioni al riguardo sono disponibili sul sito https://www.cyber-safe.ch/ (in francese e tedesco).

Figura 6: Il marchio di qualità cyber-safe.ch

4.2 Promozione di ricerca e formazione

Nel campo d'azione 1 «Acquisizione di competenze e conoscenze» sono stati compiuti progressi importanti. Tramite l'esame di professione di Cyber Security Specialist recentemente introdotto, viene creato un nuovo profilo professionale che contribuisce a contrastare la carenza di personale specializzato. Il progetto è stato portato avanti dall'esercito quale parte integrante dei lavori in preparazione di un ciclo di studi interno nel settore ciber e rappresenta un valido esempio di collaborazione costruttiva tra servizi civili e militari.
Un altro traguardo ragguardevole è l'apertura del centro di competenza tecnico-scientifico Cyber Defense Campus (poli dei due politecnici federali e polo di Thun). Il campus contribuirà a ottimizzare il trasferimento di conoscenze tra le autorità e il mondo universitario e ad affermare un proficuo ecosistema della cibersicurezza in Svizzera. Lo Swiss Support Centre for Cyber-Security dei due politecnici federali, attualmente in fase di costituzione, apporta un contributo altrettanto importante. Questo centro funge da punto di contatto tra la Confederazione e i Cantoni e svolge quindi un ruolo coordinativo.

4.2.1 Esame di professione per Cyber Security Specialist

L'11 novembre 2019, l'associazione ICT-Formazione professionale Svizzera ha presentato il nuovo esame di professione per Cyber Security Specialist (CSS)[7]. L'esame di professione con attestato professionale federale rappresenta il primo titolo di livello terziario nell'ambito della formazione professionale. Sono ammessi all'esame i candidati che hanno assolto una formazione professionale di base con attestato federale di capacità e che hanno maturato almeno due anni di esperienza professionale nel settore della sicurezza informatica o della cibersicurezza.
L'esame per CSS, co-finanziato dall'esercito, intende fornire un ulteriore incentivo ai soldati affinché seguano il ciclo di studi dell'esercito nel settore ciber. I partecipanti che concludono con successo questo ciclo di studi possono sostenere l'esame di professione se hanno maturato almeno un anno di esperienza professionale nel settore della sicurezza informatica o della cibersicurezza.

[6] Rappresentanti delle PMI: Fédération des Entreprises Romandes Neuchâtel, Chambre de commerce, d'industrie et des services de Genève, Fédération Patronale et Economique Fribourg, Chambre vaudoise du commerce et de l'industrie, Chambre valaisanne de commerce et d'industrie, Associazione svizzera dei quadri, Association Femmes PME Suisse romande, Groupement Suisse de l'Industrie Mécanique.
Altri rappresentanti: società civile (ONG ICON), scuole universitarie/università/politecnici (Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud, HES-SO Valais-Wallis, Center for Digital Trust del PFL), Comuni (Union des Communes Vaudoises).

[7] Maggiori informazioni: https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/cyber-security-specialist-efa/ (in tedesco e francese).

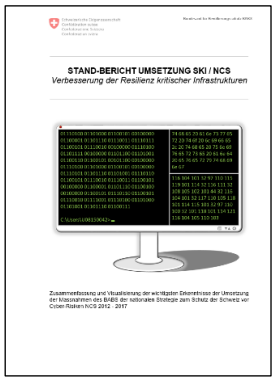
4.2.2 Cyber Defense Campus

Il Cyber Defense Campus (CYD Campus), operativo da gennaio 2019 sotto il coordinamento di armasuisse S+T, è stato costituito allo scopo di riconoscere possibilmente in modo tempestivo l'evoluzione nel settore ciber, sviluppare ed esaminare le cibertecnologie nonché assicurare la formazione e la formazione continua del personale specializzato. Il CYD Campus funge da anello di congiunzione tra le autorità, l'industria e la scienza per quanto attiene a ricerca, sviluppo e formazione nel settore della ciberdifesa. Oltre al polo di Thun, il CYD Campus ha due poli presso il PFL e il PFZ, aperti rispettivamente a settembre e a novembre del 2019.
Il CYD Campus organizza, a cadenza regolare, conferenze su tematiche che vertono sulla ciberdifesa e, in collaborazione con il PFL, offre programmi di fellowship a sostegno dell'attività di ricerca in questo ambito.

4.2.3 Swiss Support Centre for Cyber-Security e corso di master dei politecnici federali

I due politecnici federali hanno unito gli sforzi per dare vita allo Swiss Support Centre for Cyber-Security (SSCC). Il centro intende promuovere lo scambio tra i ricercatori dei politecnici federali e le autorità e fare in modo che la ricerca di punta condotta in entrambi gli istituti apporti miglioramenti concreti alla cibersicurezza della Svizzera. La questione del finaziamento del centro è stata regolata e i primi due collaboratori sono entrati in servizio. Lo SSCC sarà ampliato e fornirà vari contributi, descritti in dettaglio nel piano di attuazione della SNPC.
Infine, a partire dall'anno accademico 2019/2020 i due politecnici federali offrono un corso di master congiunto in cibersicurezza. Le materie di studio comprendono crittografia, sicurezza di hardware, software e reti, metodi per garantire la sicurezza dei sistemi e la fiducia degli utenti. Il corso di master prevede altresì parti pratiche e tratta non solo aspetti prettamente tecnici della cibersicurezza, bensì anche aspetti di carattere etico, giuridico e operativo attinenti al settore.

4.3 Resilienza delle infrastrutture critiche


STAND-BERICHT UMSETZUNG SKI / NCS
Verbesserung der Resilienz kritischer Infrastrukturen

Zusammenfassung und Visualisierung der wichtigsten Erkenntnisse der Umsetzung der Massnahmen des BABS der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS 2012 - 2017

Sulla base delle analisi dei rischi e delle vulnerabilità svolte nel periodo 2012–2017, l'UFPP ha redatto un rapporto sullo stato di resilienza delle infrastrutture critiche della Svizzera. Il rapporto presenta la situazione attuale dei rischi stimati e le misure in corso per migliorare la resilienza. I risultati ottenuti servono a classificare meglio i ciber-rischi nell'ambito di una situazione globale di pericolo delle infrastrutture suddette. Inoltre, le informazioni aggregate consentono di individuare problematiche di carattere generale e quindi di sfruttare meglio le sinergie nella fase di elaborazione.

Figura 7: Rapporto sullo stato di resilienza delle infrastrutture critiche

Per i responsabili delle decisioni, i risultati ottenuti fungono da base per prioritizzare possibili misure di resilienza nei settori parziali critici.

Nel quadro dell'attuazione della seconda SNPC 2018–2022 sarà effettuato, sotto la guida dell'UFPP, un aggiornamento delle analisi dei rischi e delle vulnerabilità esistenti da cui, se necessario, saranno desunte nuove misure per migliorare la resilienza. Quelle decise nel

quadro della prima SNPC e in corso di attuazione proseguono invariate.

4.4 Standardizzazione

Per quanto riguarda il campo d'azione «Standardizzazione / regolamentazione», è stato redatto un rapporto sullo standard di sicurezza per i dispositivi IoT e sono stati elaborati altri standard minimi per i settori critici.

4.4.1 Standard di sicurezza per i dispositivi IoT

Il rapporto sullo standard di sicurezza per i dispositivi IoT spiega le sfide correlate alla sicurezza dei sistemi con componenti IoT, gli standard internazionali applicabili per la protezione di questi sistemi e le basi legali vigenti in Svizzera. Il rapporto, redatto in adempimento del postulato Glättli 17.4295 del 15.12.2017 e del postulato Reynard 19.3199 del 21.3.2019[8], intende fungere da base per i futuri lavori in questo settore.

4.4.2 Standard minimi TIC

Gli standard minimi TIC vanno intesi come raccomandazione e possibile riferimento per migliorare la resilienza TIC delle imprese. Sono pensati in modo particolare per i gestori di infrastrutture critiche, ma in linea di principio possono essere applicati da qualsiasi impresa e organizzazione, che ne possono disporre liberamente[9].

Per facilitare l'applicazione degli standard minimi nei settori critici, le associazioni di categoria allestiscono i rispettivi standard specifici in collaborazione con l'UFAE. Tali standard sono già stati approntati per i settori energia elettrica, derrate alimentari, approvvigionamento idrico e acque di scarico.

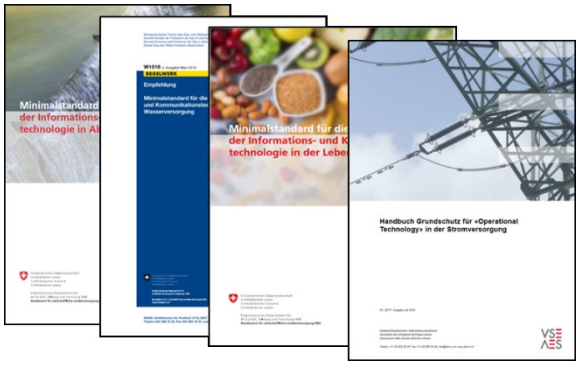


Figura 8: Standard minimi TIC

4.5 Verifica dell'obbligo di notifica

Nel dicembre del 2019 il Consiglio federale ha approvato il rapporto sulle varianti per l'attuazione di un obbligo di notifica in caso di gravi incidenti legati alla sicurezza delle infrastrutture critiche[10]. Il rapporto, in adempimento del postulato 17.3475 Graf-Litscher, indica possibili varianti per l'introduzione dell'obbligo di notifica. Queste sono state concepite basandosi sugli obblighi di notifica esistenti per gli incidenti legati alla sicurezza, sulle conclusioni tratte dalle interviste con esperti e sulle analisi degli obblighi di notifica vigenti in altri Paesi. Nell'ambito delle possibili varianti è fondamentale chiarire se i ciberincidenti devono essere segnalati a una centrale separata o se è necessario incrementare le centrali d'annuncio in parte già operanti nei diversi settori. A seconda di questa struttura organizzativa bisogna valutare a partire da quale entità e a quali condizioni vige l'obbligo di notifica dei ciberincidenti, le scadenze applicabili per la notifica, la possibilità di effettuare notifiche anonime e l'ipotesi di stabilire sanzioni per le omissioni. Il Consiglio federale ha

[8] https://www.ncsc.admin.ch/melani/de/home/dokumentation/berichte.html (in tedesco e francese)

[9] https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html

[10] https://www.ncsc.admin.ch/melani/de/home/dokumentation/berichte.html (in tedesco e francese)

incaricato il NCSC e l'UFPP di chiarire questi aspetti coinvolgendo le autorità competenti dei Cantoni, della Confederazione e dell'economia. È necessario altresì esaminare la possibilità di estendere l'obbligo di notifica generale agli incidenti legati alla perdita della capacità di funzionamento delle infrastrutture critiche. Entro la fine del 2020 il Consiglio federale intende prendere le decisioni di principio in merito all'introduzione di tali obblighi.

4.6 Migliore coordinamento nella lotta alla cibercriminalità

Con l'istituzione del Cyberboard, le autorità preposte al perseguimento penale hanno stabilito, in collaborazione con le autorità partner, un metodo di lavoro per il trasferimento delle conoscenze e il coordinamento strategico-operativo nella lotta alla cibercriminalità a livello nazionale. Il Cyberboard è costituito dall'organo direttivo-strategico Cyber-STRAT e da altri gruppi operativi, formati dal Cyber-CORE (elemento centrale che svolge compiti coordinativi), dal Cyber-CASE (panoramica dei casi) e dal Cyber-STATE (rappresentazione della situazione). Dal 2019 il Cyberboard riunisce regolarmente le principali autorità di perseguimento penale attive nella lotta alla cibercriminalità, in particolare gli specialisti della Rete di sostegno alle indagini nella lotta contro la criminalità digitale (NEDIK). L'anno scorso questo ha permesso di intensificare la collaborazione, segnatamente di prevenire l'insorgenza di controversie sul foro competente nelle questioni di competenza problematiche e di giungere rapidamente a soluzioni amichevoli, il che giova a contrastare la cibercriminalità.
Inoltre, come base per la collaborazione a livello operativo, ogni Ministero pubblico ha nominato un Single Point of Contact (SPOC) ciber. Nel quadro di questa collaborazione, le autorità di perseguimento penale hanno perfezionato il coordinamento a livello nazionale per determinati eventi, ad esempio gli annunci immobiliari fasulli o gli attacchi di ransomware sferrati alle imprese. La collaborazione in materia di polizia è promossa in seno a NEDIK, una rete ormai consolidata che sarà ulteriormente ampliata. Per l'accertamento sistematico dei casi, un gruppo di Cantoni della Svizzera occidentale ha sviluppato la Plateforme d'Information de la Criminalité Sérielle en Ligne (PICSEL), al momento in fase di test. In tal modo le autorità di perseguimento penale dispongono dei presupposti essenziali per potenziare costantemente, nell'ambito della collaborazione congiunta, le capacità di contrastare la cibercriminalità e per attuare le misure della SNPC.

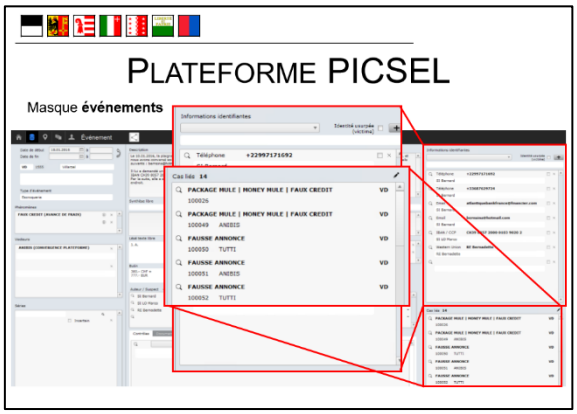


Figura 9: Piattaforma PICSEL

4.7 Collaborazione rafforzata con i Cantoni

Dopo la decisione del Consiglio federale di istituire un centro nazionale per la cibersicurezza, diversi Cantoni hanno espresso l'interesse di farne parte e offerto il loro sostegno. Nei primi colloqui con i Cantoni tenutisi nel 2019 sono stati illustrati possibili modi per coordinare meglio il lavoro della Confederazione con le competenze esistenti a livello cantonale nel settore della cibersicurezza.
Successivamente, a marzo 2020 la piattaforma politica della RSS ha incaricato il suo delegato di tracciare un bilancio delle competenze e dei progetti cantonali per avere un

quadro della situazione e per gettare le basi in vista di una collaborazione strutturata tra il NCSC e i Cantoni.

4.8 Rinnovo del partenariato pubblico-privato Swiss Cyber Experts

Nel primo trimestre del 2020 è stato firmato il nuovo contratto di cooperazione tra la Confederazione e l'associazione Swiss Cyber Experts (SCE), con l'opzione di prolungare il contratto per altri cinque anni. L'associazione fornirà supporto al NCSC nell'analisi degli incidenti, contribuirà a fornire un quadro della situazione della Confederazione e, se necessario, a svolgere altri compiti di supporto a favore della cibersicurezza in Svizzera.

Figura 10: Logo di Swiss Cyber Experts

4.9 Geneva Dialogue on Responsible Behaviour in Cyberspace

Nella Strategia di politica estera 2020–2023[11], il Consiglio federale riconosce la digitalizzazione quale una delle priorità tematiche della politica estera della Svizzera. In questo contesto, la ciberdiplomazia è definita come elemento cardine della politica estera digitale. Obiettivo della ciberdiplomazia è tutelare gli interessi della Svizzera nel ciberspazio (ovvero nello spazio digitale). Al proposito, il nostro Paese intende consolidare il suo impegno internazionale e profilarsi in modo più incisivo nel settore della ciberdiplomazia.
Il progetto Geneva Dialogue on Responsible Behaviour in Cyberspace è parte integrante di queste attività. Lanciato alla fine del 2018 come progetto congiunto di DiploFoundation, Istituto di ricerca delle Nazioni Unite sul disarmo (UNIDIR), PFZ e Università di Losanna, nel maggio del 2020 è entrato nella seconda fase. In essa, il dialogo tra le aziende globali è incentrato sulle buone pratiche volte a incrementare la sicurezza dei prodotti nel ciberspazio. Oltre ad aziende svizzere di fama mondiale come UBS e SwissRe, vi partecipano anche Microsoft (Stati Uniti), Cisco (Stati Uniti), Kaspersky (Russia), Sberbank (Russia), Huawei (Cina), Siemens (Germania), FireEye (Stati Uniti) e VU Security (Argentina). Il progetto è realizzato dal DFAE in collaborazione con WEF, PFZ e Swiss Digital Initiative.

[11] https://www.eda.admin.ch/eda/it/dfae/dfae/attuazione-politica-estera/aussenpolitischestrategie.html

5 Stato di attuazione: quadro dettagliato

Di seguito è presentato lo stato di attuazione della SNPC in relazione alla pianificazione delle tappe fondamentali. Per ciascuna misura sono raffigurate le tappe fondamentali attuate e quelle non attuate nel primo trimestre del 2020. Segue una loro breve descrizione esplicativa.
Su un totale di 247 tappe fondamentali contenute nel piano di attuazione della SNPC, 72 di queste sono state attuate, 23 sono state rimandate[12] e 3 non sono state attuate. Con uno stato di attuazione di quasi un terzo a conclusione di 9 su 20 trimestri di durata complessiva della SNPC, si può affermare che la strategia è a buon punto, anche se per la maggioranza delle misure il grosso del lavoro deve ancora iniziare. La figura 11 mostra lo stato di attuazione di tutte le tappe fondamentali.

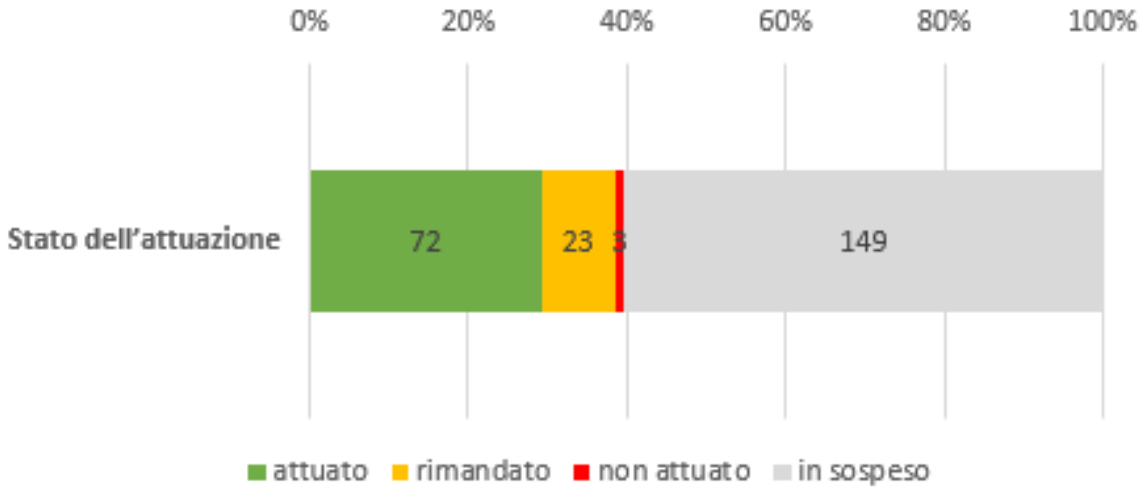


Figura 11: Stato di attuazione delle tappe fondamentali della SNPC

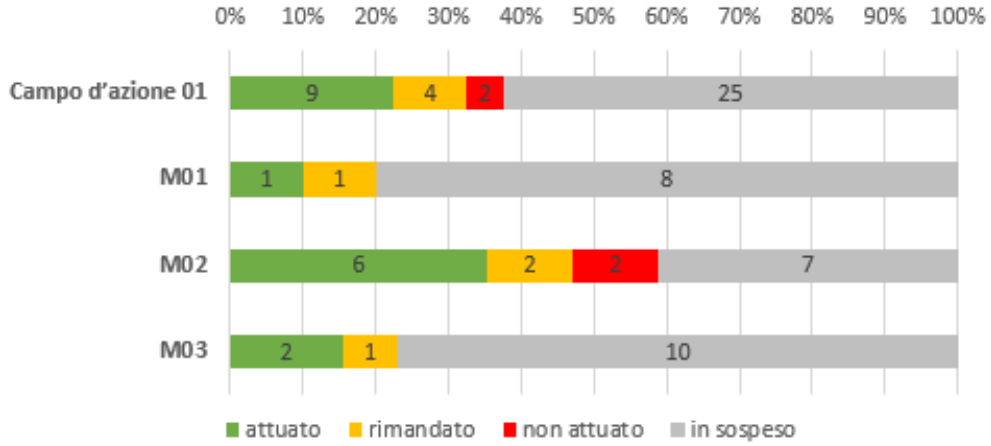
[12] È il caso quando una tappa fondamentale non è stata realizzata per tempo, ma i responsabili dell'attuazione possono documentare in modo plausibile che quest'ultima non è compromessa.

5.1 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 primo trimestre 2020

	Tappa fondamentale	Stato
M1	Monitoraggio delle tecnologie: le prestazioni del CYD Campus per il monitoraggio all'attenzione del NCSC sono stabilite	Attuato
	Analisi delle tendenze: il piano per il pubblico target e i contenuti sono elaborati, i rapporti sono trasmessi	Rimandato
M2	Analisi del fabbisogno per la creazione di offerte formative: l'analisi è effettuata e i gruppi target sono definiti	Rimandato
	Centro di ricerca e supporto dei due politecnici federali: il relativo piano è allestito	Attuato
	Centro di ricerca e supporto dei due politecnici federali: gli aspetti riguardanti il finanziamento e l'ubicazione sono chiariti	Attuato
	Il CYD Campus (polo di Thun) è operativo	Attuato
	Il CYD Campus (polo del PFL) è operativo	Attuato
	Il CYD Campus (polo del PFZ) è operativo	Attuato
	I principali istituti di ricerca nel settore dei ciber-rischi sono identificati	Rimandato
	Gli eventi consolidati in materia di hackeraggio etico sono identificati	Attuato
	Gli strumenti di promozione sono predisposti; la domanda di finanziamento, laddove necessario, è presentata e i mezzi finanziari sono disponibili	Non attuato. Misura: modifica del progetto. Il finanziamento tramite la Confederazione non è il mezzo adatto per promuovere eventi in materia di hackeraggio etico.
M3	Ecosistema della cibersicurezza: i principali istituti di ricerca nel settore dei ciber-rischi sono identificati	Rimandato

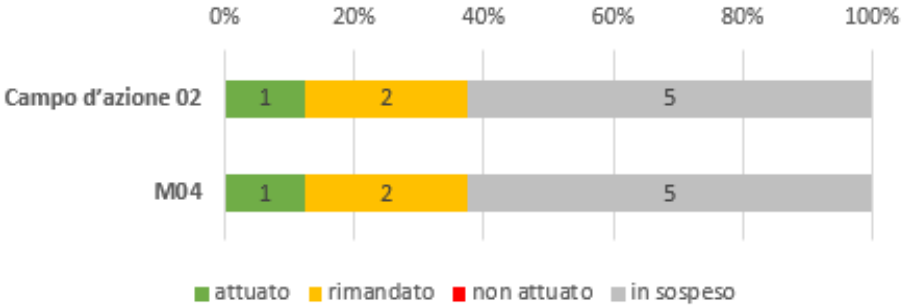
	Think Tank: il piano per il centro di ricerca e supporto dei due politecnici federali è allestito	Attuato
	Think Tank: gli aspetti riguardanti il finanziamento e l'ubicazione del centro di ricerca e supporto dei due politecnici federali sono chiariti	Attuato

5.2 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 ciberminacce (SIC)

Stato di attuazione



Tappe fondamentali dal 2018 al primo trimestre 2020

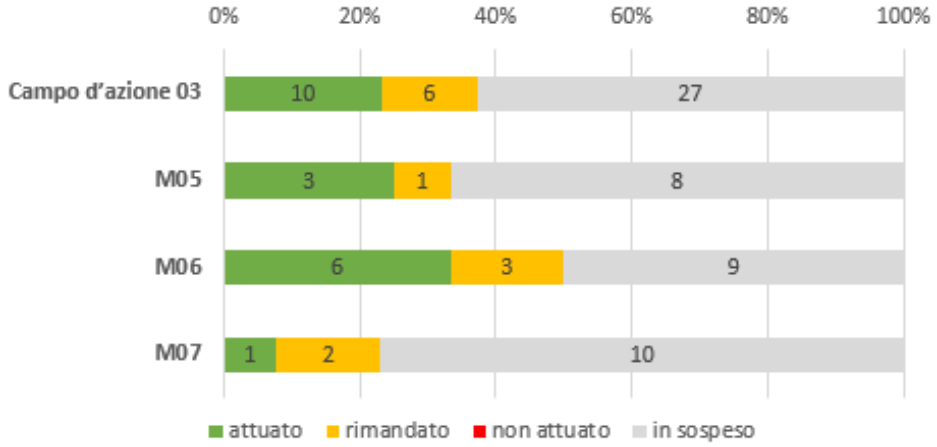
	Tappa fondamentale	Stato
M4	L'analisi del fabbisogno è effettuata e i gruppi target sono definiti	Attuato
	Catalogo delle prestazioni: l'ambito di competenza della Confederazione e del mondo economico è chiarito	Rimandato
	Fonti: l'elenco delle ulteriori fonti necessarie è redatto	Attuato

5.3 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[13])

Stato di attuazione



Tappe fondamentali dal 2018 al primo trimestre 2020

	Tappa fondamentale	Stato
M5	L'inventario delle disposizioni attuate e di quelle non ancora attuate contemplate dai rapporti sulle misure è redatto	Attuato
	Le responsabilità per l'attuazione sono chiarite	Attuato
	La tabella di marcia e la pianificazione delle misure in atto e imminenti è elaborata	Attuato
	Il gruppo di lavoro accademico per la cibersicurezza è costituito	Rimandato
M6	Direttive in materia di sicurezza: i compiti attuali e i risultati rilevanti ai fini della sicurezza nei metodi di progetto sono analizzati	Rimandato
	Il piano di massima della campagna di sensibilizzazione per la sicurezza informatica nell'Amministrazione federale «IKT Security 19» è allestito (T4/2018)	Attuato
	La campagna di sensibilizzazione per la sicurezza informatica nell'Amministrazione federale «IKT Security» è avviata	Attuato
	Armonizzazione con gli attori attivi per l'estensione del piano a una campagna nazionale (cfr. M29 «Sensibilizzazione del pubblico sui rischi informatici»)	Rimandato
	Allestimento di un ulteriore piano di misure di sensibilizzazione per gli anni 2021/2022	Rimandato

[13] Maggiori informazioni su altri progetti concernenti il piano di attuazione dei Cantoni relativo alla Strategia nazionale per la protezione della Svizzera contro i ciber-rischi 2018–2022, elaborato dalla RSS, nonché sul rispettivo stato di attuazione sono reperibili qui (in tedesco e francese): https://www.svs.admin.ch/content/svs-internet/de/themen-/cybersicherheit/cybersicherheit-kantone/_jcr_content/contentPar/downloadlist_1137108093/downloadItems/145_1588841512416.download/Jahresbericht%20zum%20Stand%20der%20Projekte%20im%20Umsetzungsplan%20der%20Kantone.pdf

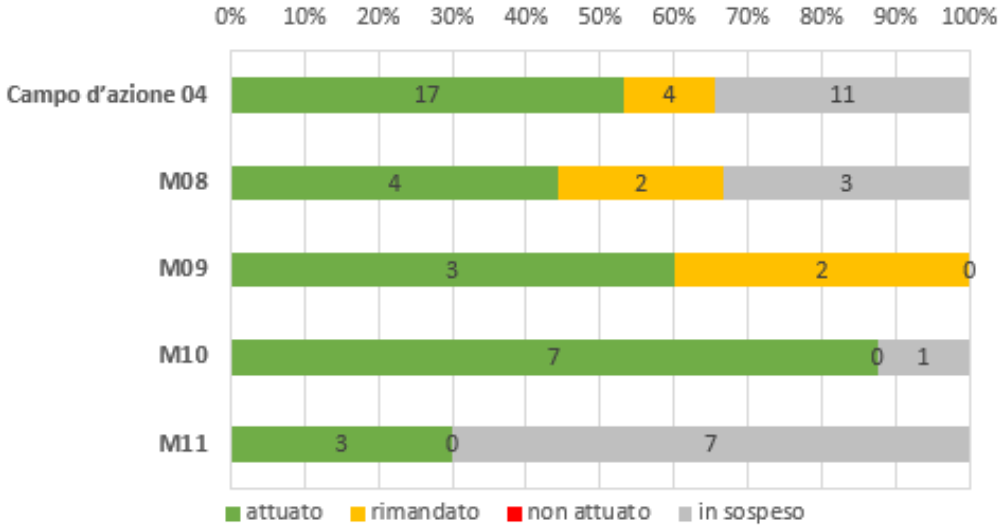
	SCION: dichiarazione d'intenti di utenti interessati e partecipanti alla fase pilota	Attuato
	SOC: progetto e piano di attuazione	Attuato
	SOC: la fase di attuazione è conclusa	Rimandato
	Interfaccia con il PFZ: coordinamento con il delegato alla cibersicurezza	Attuato
M7	Scambio di conoscenze con i Cantoni: accertamento dei requisiti della dotazione del posto di lavoro presso il NCSC	Rimandato
	Svolgimento dell'incontro annuale nazionale Cyber-Landsgemeinde	Attuato
	Interfaccia tra PFZ e Cantoni: coordinamento con la RSS	Rimandato

5.4 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 primo trimestre 2020

	Tappa fondamentale	Stato
M8	Pubblicazione dello standard minimo TIC e strumenti per l'assessment	Attuato
	Standard minimo secondo il manuale per la protezione di base «Handbuch Grundschutz» (in tedesco e francese) dell'Associazione delle aziende elettriche svizzere	Attuato
	Standard dei settori approvvigionamento idrico e derrate alimentari	Attuato
	Standard del settore gas naturale	Rimandato
	Standard del settore trasporti pubblici	Rimandato
	Pubblicazione del test di cibersicurezza online per le PMI (SATW) nel terzo trimestre del 2018	Attuato

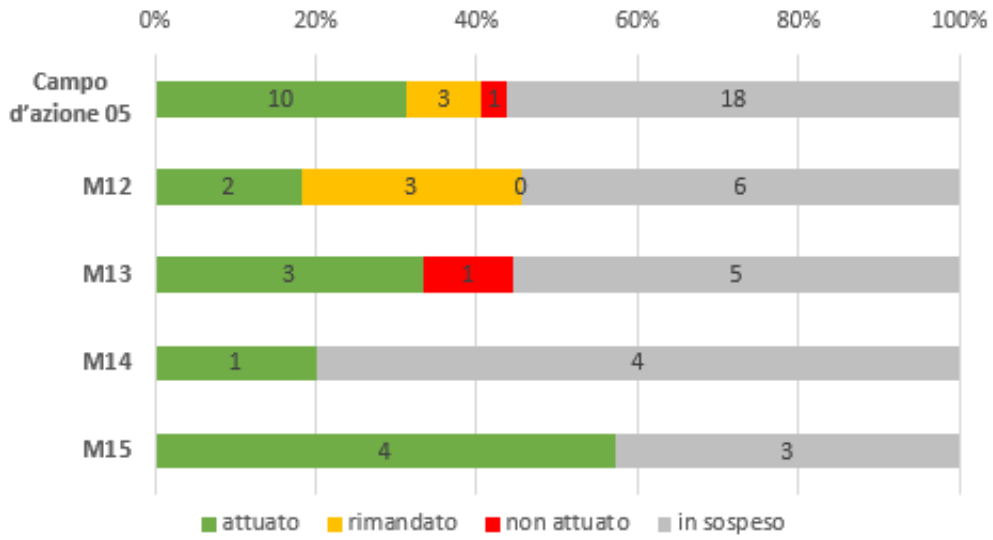
	Analisi del fabbisogno di altri strumenti (ausili tecnici, marchi di qualità, guide, istruzioni) per le PMI	Attuato
M9	Messa a concorso ed elaborazione dello studio di base	Attuato
	Rapporto (postulato)	Attuato
	Prosieguo del dibattito con i rappresentanti della politica e dell'economia	Rimandato
	Base per la decisione di introdurre l'obbligo di notifica	Rimandato
M10	Incontro del gruppo di alto livello istituito dal Segretario generale delle Nazioni Unite (New York, Ginevra, Helsinki)	Attuato
	Rapporto del gruppo di alto livello	Attuato
	Valutazione delle possibilità di attuazione del rapporto	Attuato
M11	Pool di esperti: accertamento del fabbisogno	Attuato
	Pool di esperti: creazione di posti per il pool	Attuato
	Il progetto del centro comune di ricerca e supporto PFL-PFZ è elaborato	Attuato

5.5 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 primo trimestre 2020

	Tappa fondamentale	Stato
M12	CUG di MELANI: l'analisi della situazione in merito all'utilizzo di MELANI da parte dei diversi settori critici è effettuata	Rimandato
	Lo studio con le varianti raccomandate di MELANI-NET 2.0 è redatto (T3/2018)	Attuato
	La prova di fattibilità in merito alla variante raccomandata è effettuata	Attuato

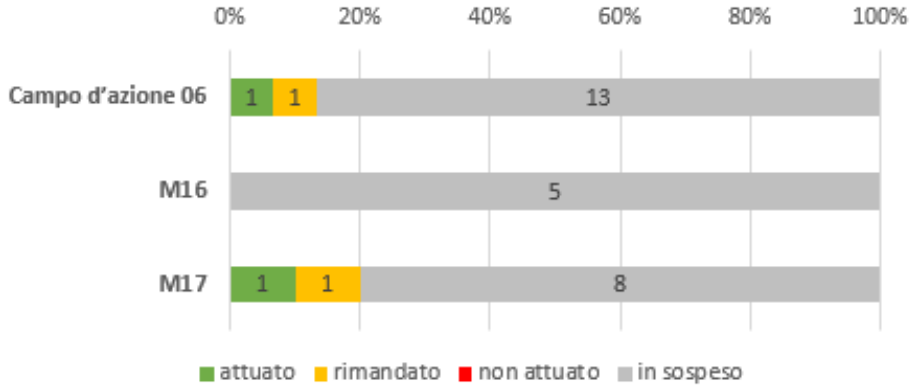
	Piano MELANI-NET 2.0	Rimandato
	Il piano MELANI-NET 2.0 è operativo	Rimandato
M13	Servizio nazionale di contatto ciber: il piano di massima del portale online per la segnalazione di incidenti informatici è allestito	Attuato
	L'analisi della situazione e del fabbisogno di possibili buone pratiche per la gestione degli incidenti è effettuata	Non attuato. Misura: nuova pianificazione del progetto e coinvolgimento di altri partner.
	Accertamento delle esigenze di allarme, allerta e informazione del pubblico in caso di incidente informatico > app Alertswiss	Attuato
	Il piano di integrazione delle ciberinformazioni nella app Alertswiss è allestito	Attuato
M14	Il censimento dei SOC e dei CERT attualmente operativi, inclusi i rispettivi interlocutori, è realizzato e documentato	Attuato
M15	Elaborazione dell'ordinanza sui ciber-rischi	Attuato
	Approvazione dell'OCiber da parte del Consiglio federale	Attuato
	L'entrata in vigore dell'OCiber è fissata	Attuato
	Prima bozza di una procedura per la gestione delle crisi nell'Amministrazione federale, discussione con i fornitori di prestazioni e i servizi coinvolti	Attuato

5.6 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 primo trimestre 2020

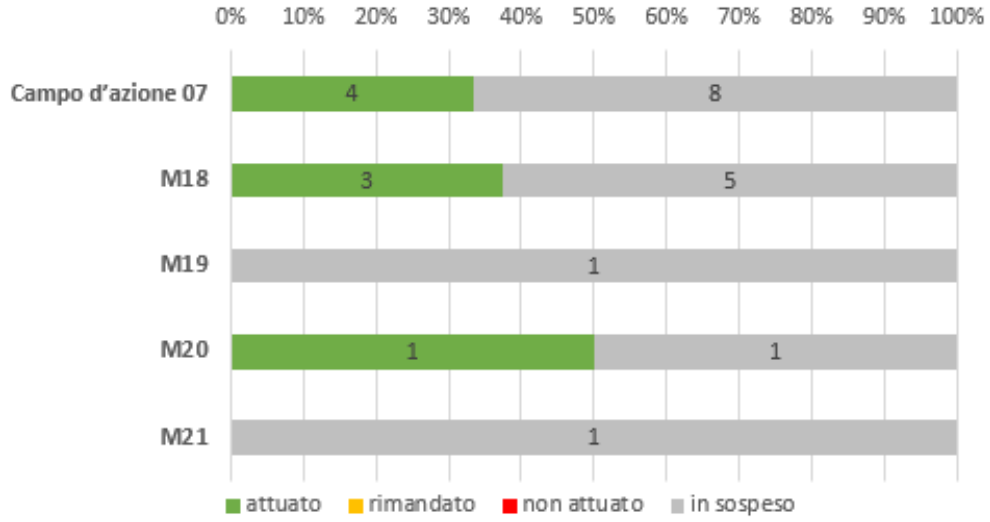
	Tappa fondamentale	Stato
M16	Nessuna tappa fondamentale entro il primo trimestre del 2020	
M17	Inventario delle esercitazioni di crisi nazionali e internazionali in essere e previste che implicano aspetti inerenti al ciberspazio	Rimandato
	L'analisi del fabbisogno di esercitazioni in caso di crisi in settori specifici è effettuata	Attuato

5.7 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 primo trimestre 2020

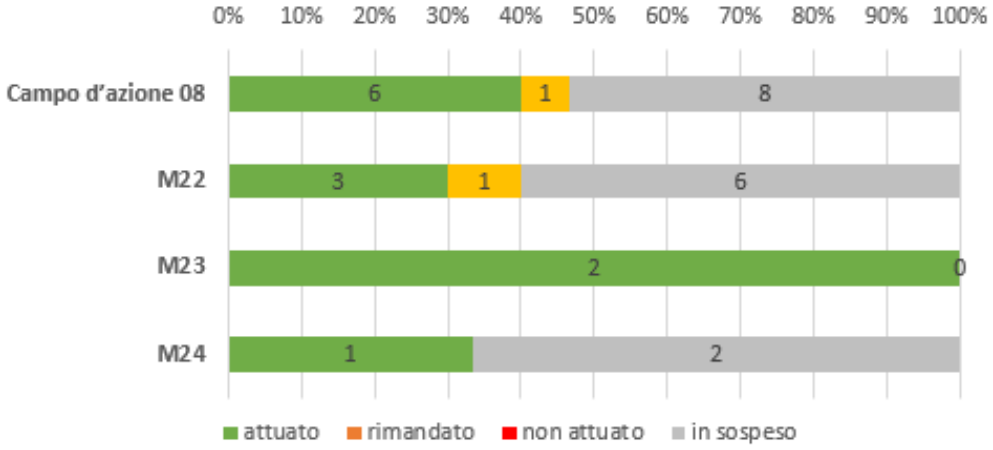
	Tappa fondamentale	Stato
M18	Panoramica dei casi in materia di criminalità informatica: avviata la fase di test PICSEL	Attuato
	Software Cyber-CASE; elenco della serie di casi di tutti gli SPOC ciber dei Ministeri pubblici (già operativo)	Attuato
	Bollettino mensile (della polizia) NEDIK	Attuato
M19	Nessuna tappa fondamentale entro il primo trimestre del 2020	
M20	Panoramica delle possibilità di formazione a livello accademico (della polizia)	Attuato
M21	Nessuna tappa fondamentale entro il primo trimestre del 2020	

5.8 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 primo trimestre 2020

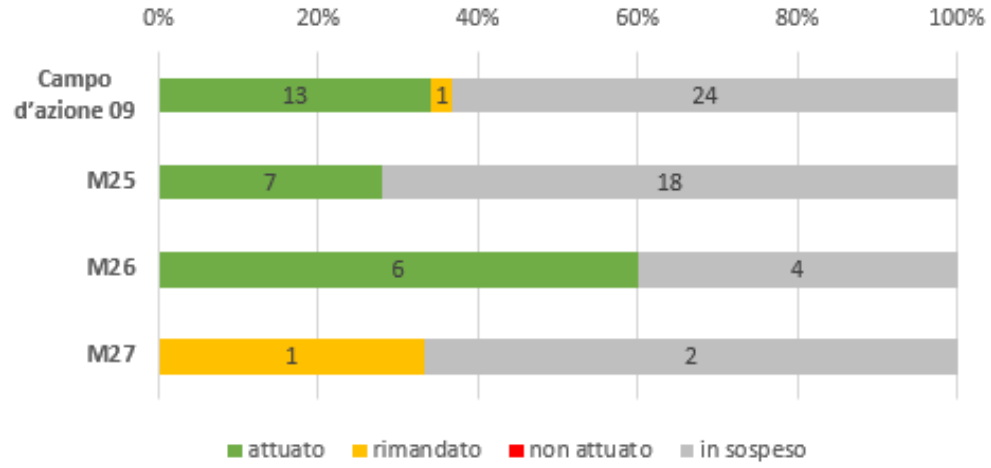
	Tappa fondamentale	Stato
M22	Ampliamento delle capacità di acquisizione delle informazioni e di attribuzione degli attacchi informatici: la prima tappa dell'ampliamento è realizzata	Rimandato
	Formazione: prima esercitazione con la BAC delle Forze terrestri	Attuato
	Avvio del corso di master congiunto PFL-PFZ-DDPS	Attuato
	Primi corsi organizzati dal PFL e dal DDPS	Attuato
M23	Capacità BAC-CEO: le attività previste sono state discusse con gli uffici specializzati in merito a effetti collaterali indesiderati	Attuato
	Le capacità sono disponibili	Attuato
M24	Conclusione del progetto pertinente	Attuato

5.9 Posizionamento attivo della Svizzera nella politica di cibersicurezza 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 primo trimestre 2020

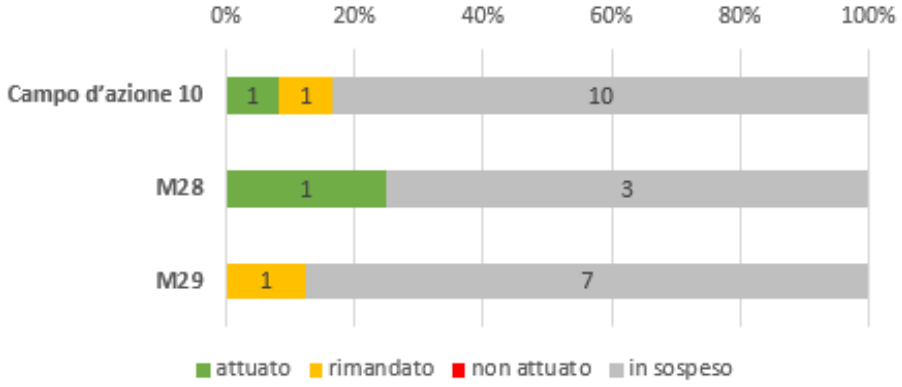
	Tappa fondamentale	Stato
M25	Partecipazione ai processi dell'ONU: rapporto annuale	Attuato
	OCSE: adesione ai negoziati, partecipazione attiva al processo e rapporto annuale	Attuato
	Piano per l'istituzione del Geneva Dialogue come piattaforma multistakeholder	Attuato
	Due-tre tornate di dialogo del processo di esperti in merito all'applicazione del diritto internazionale pubblico nel ciberspazio hanno avuto luogo	Attuato
	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	Attuato
	Quadro dei processi riguardanti i diritti dell'uomo e dei forum rilevanti	Attuato
M26	Cooperazione internazionale: preparazione del piano e svolgimento del primo workshop a Ginevra	Attuato
	Organizzazione di workshop per la creazione di istituzioni e strutture in materia di cibersicurezza esterna: analisi del fabbisogno, esercitazioni, piano, svolgimento del primo workshop	Attuato
M27	Sino-European Cyber Dialogue (SECD): continuazione dei lavori	Rimandato

5.10 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 primo trimestre 2020

	Tappa fondamentale	Stato
M28	Piano per la comunicazione del NCSC: l'analisi della situazione è effettuata	Attuato
M29	La concertazione con altri attori attivi sull'elaborazione concettuale di una campagna di sensibilizzazione nazionale è avvenuta	Rimandato