La Strategia Ciber DDPS

in sintesi

Marzo 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Sintesi della Strategia Ciber DDPS

Così la Svizzera protegge nel ciberspazio

Il Consiglio federale affronta attivamente i ciber-rischi e adotta le misure necessarie per salvaguardare la sicurezza del Paese dalle minacce provenienti dal ciberspazio.

Dal 2012 la Svizzera dispone di una **Strategia nazionale per la protezione della Svizzera contro i ciber-rischi** (SNPC), al fine di gestire le opportunità e le sfide nel ciberspazio. Nel 2018 la Strategia è stata ampliata con misure supplementari; è stata inoltre sottolineata l'importanza della collaborazione tra la Confederazione, i Cantoni, i partner dell'economia e le scuole universitarie. La Strategia tiene conto della crescente digitalizzazione e interconnessione della società e dell'amministrazione. Responsabile a livello di Confederazione è il delegato alla cibersicurezza presso il Centro nazionale per la cibersicurezza (National Cyber Security Centre – NCSC) in seno al Dipartimento federale delle finanze (DFF).

*Con **ciberspazio** si intende uno spazio virtuale creato da persone mediante mezzi TIC. Serve all'interconnessione e all'elaborazione digitali di dati nonché al rilevamento e alla gestione di sistemi e processi.*

*Le misure di protezione contro i ciber-rischi sono suddivise nei seguenti settori (secondo l'art. 6 dell'ordinanza sui ciber-rischi): cibersicurezza, **ciberdifesa** e cibercriminalità.*

Chi è protetto?

Da un lato, assume un ruolo centrale la protezione delle cittadine e dei cittadini contro la criminalità nel ciberspazio. Dall'altro lato, le infrastrutture critiche devono essere protette da perturbazioni e danni provocati, intenzionali e involontari che possono colpire la popolazione, l'economia e l'amministrazione. In caso di ciberattacchi su larga scala, per esempio a causa di intenzioni malevole da parte di uno Stato, si ricorre alla ciberdifesa. Quest'ultima comprende diversi mezzi del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e protegge la Svizzera, la sua popolazione nonché le sue basi vitali contro ciberminacce. Anche in caso di ciberperturbazioni maggiori, non causate con intenzioni malevole, la ciberdifesa può essere impiegata quale supporto.

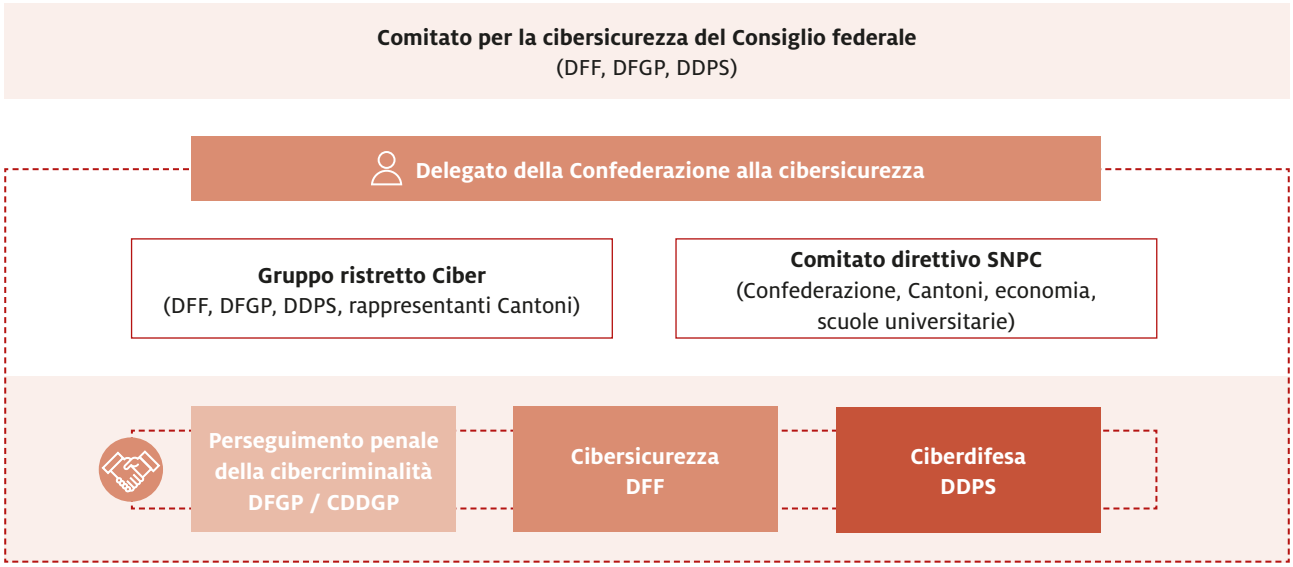


Figura 1 – Responsabilità per la cibersicurezza nell'Amministrazione federale

Così protegge il DDPS nel ciberspazio: in modo strategico, integrato, permanente

Finora: dal 2017 al 2020

Il **Piano d'azione Ciberdifesa DDPS (PACD)** del 2017 definisce in modo specifico, quale parte integrante della SNPC, i compiti, le competenze e i processi delle unità amministrative del DDPS nella gestione della ciberdifesa. Le misure stabilite in tale contesto sono state ampiamente attuate entro la fine del 2020.

Con il **coordinamento di competenze e capacità** il DDPS ha guadagnato in effettività. È stato possibile migliorare la collaborazione tra i dipartimenti. Il DDPS collabora con **i Cantoni, l'economia e le scuole universitarie** nonché, se necessario, con partner internazionali. Oggi il DDPS dispone di capacità per fornire una protezione e prestazioni di difesa eccellenti nel ciberspazio e può ricorrere a una rete affidabile in Svizzera e all'estero.

Oggi: dal 2021 al 2024

La **Strategia Ciber DDPS** si fonda sulle conoscenze evinte dal Piano d'azione Ciberdifesa. Garantisce che il DDPS e le sue unità amministrative siano orientati in modo mirato e sistemico alle esigenze in costante evoluzione.

La **Strategia Ciber DDPS** riflette, in una prima fase, sulla situazione di minaccia, sulle sfide e sulle tendenze nel ciberspazio a livello mondiale.[1] Vengono descritti gli sviluppi attesi prossimamente nei settori della tecnologia, della politica, dell'economia e del personale.

Per esempio, le azioni malevole vengono automatizzate in misura crescente ed eseguite basandosi sull'intelligenza artificiale. Le configurazioni di sicurezza insufficienti di sistemi appartenenti a diverse generazioni (Legacy Systems) vengono sfruttate sistematicamente. La crescente importanza dei social media e la forte interconnessione digitale potrebbero determinare un ulteriore incremento dell'abuso del ciberspazio per operazioni di carattere manipolativo.

1 Vedi rapporto annuale Servizio delle attività informative della Confederazione SIC: «La sicurezza della Svizzera 2020»

La Strategia Ciber DDPS presenta un'analisi della **situazione reale.** Illustra come i compiti e le misure tratte dal PACD, il documento precedente alla Strategia, siano state concretizzate finora. Ciò comprende, ad esempio, l'ulteriore sviluppo del corso di formazione ciber della scuola reclute e il Cyberdefence-Campus di armasuisse. La Svizzera continua inoltre a partecipare a cibereserciazioni a livello internazionale.

La sincronizzazione delle minacce, delle sfide e delle tendenze con lo stato reale permette di identificare il potenziale di sviluppo futuro. Gli insegnamenti che ne derivano servono da punto di partenza per la formulazione degli obiettivi della Strategia Ciber DDPS. Quest'ultima stabilisce chi in seno al DDPS assume e assumerà quali compiti. La Strategia Ciber DDPS si concentra sul settore della ciberdifesa. La **Strategia nazionale SNCP** sovraordinata e altri documenti di riferimento coprono ulteriori aspetti della cibersicurezza.

*Con **situazione di minaccia** si intendono azioni malevole da parte di attori statali e non statali, per arricchirsi o imporre interessi politici. A tale scopo si può ricorrere allo spionaggio, al sabotaggio o alla disinformazione / destabilizzazione mirata.*

__Sfide:__ sono intesi gli sviluppi tecnologici, le dipendenze e la politica egemonica. Ciò comprende anche la penuria di risorse naturali – in particolare le terre rare o l'approvvigionamento elettrico – nonché il fabbisogno di istruzione e la carenza di specialisti.

Strategia Ciber DDPS

Contribuiamo alla protezione del Paese, lo difendiamo nel ciberspazio e aumentiamo considerevolmente la sua libertà d'azione.

È nell'interesse in materia di politica di sicurezza della Svizzera di proteggere la libertà d'azione e l'integrità dello Stato, dell'economia e della popolazione anche nel ciberspazio e di difenderli in caso di conflitto.

Il DDPS è competente per la ciberdifesa della Svizzera in collaborazione con i suoi partner presso la Confederazione e i Cantoni, l'economia e le scuole universitarie nonché, in caso di necessità, con partner internazionali. Anticipa e analizza nel quadro delle sue responsabilità le sfide e le minacce in ambito ciber, e fornisce prestazioni di sicurezza volte a gestire ciberincidenti in tempo di pace, tensioni e conflitti.

Il DDPS contribuisce (in modo sussidiario) a proteggere infrastrutture critiche contro ciberattacchi e a rafforzarne la resilienza.

__Resilienza:__ la capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni e di mantenere il più possibile la capacità di funzionamento o di ripristinarla rapidamente.

I 6 obiettivi strategici

La gestione dell'attuazione della *Strategia Ciber DDPS* ha luogo nel quadro della conferenza «Ciberdifesa DDPS». Il DDPS vuole realizzare i seguenti obiettivi:

1. **Il DDPS conosce le sfide e gli sviluppi nel ciberspazio.** Comprende le minacce, le opportunità e i rischi che ne derivano e si adegua costantemente per gestirli.
2. **Il DDPS è in grado di prevenire minacce e attacchi** che causano danni, hanno ripercussioni a livello nazionale o mettono in pericolo gli interessi nazionali.[2] Il DDPS può individuare, disturbare o impedire tempestivamente e in ogni situazione minacce e attacchi.
3. **Il DDPS offre istruzioni e perfezionamenti** per i collaboratori civili e militari nonché per i militari di milizia, al fine di prepararli alle sfide in ambito ciber.
4. Il DDPS **minimizza** la **vulnerabilità nei confronti dei ciber-rischi** ed è resistente. In caso di evento o di crisi, ripristina il più rapidamente possibile le funzioni fondamentali, è in grado di adempiere i suoi compiti ed è resiliente.
5. Il DDPS mantiene aggiornati sul piano tecnico l'hardware, i software e le reti. Provvede a un esercizio affidabile e garantisce che sia sempre disponibile il materiale necessario. Il DDPS è il più possibile indipendente da fornitori di prestazioni e fornitori in generale aumentando così la propria **autonomia.**
6. Il DDPS si posiziona nel settore della ciberdifesa assumendo un ruolo di **pioniere e modello** nonché di **datore di lavoro attrattivo.**

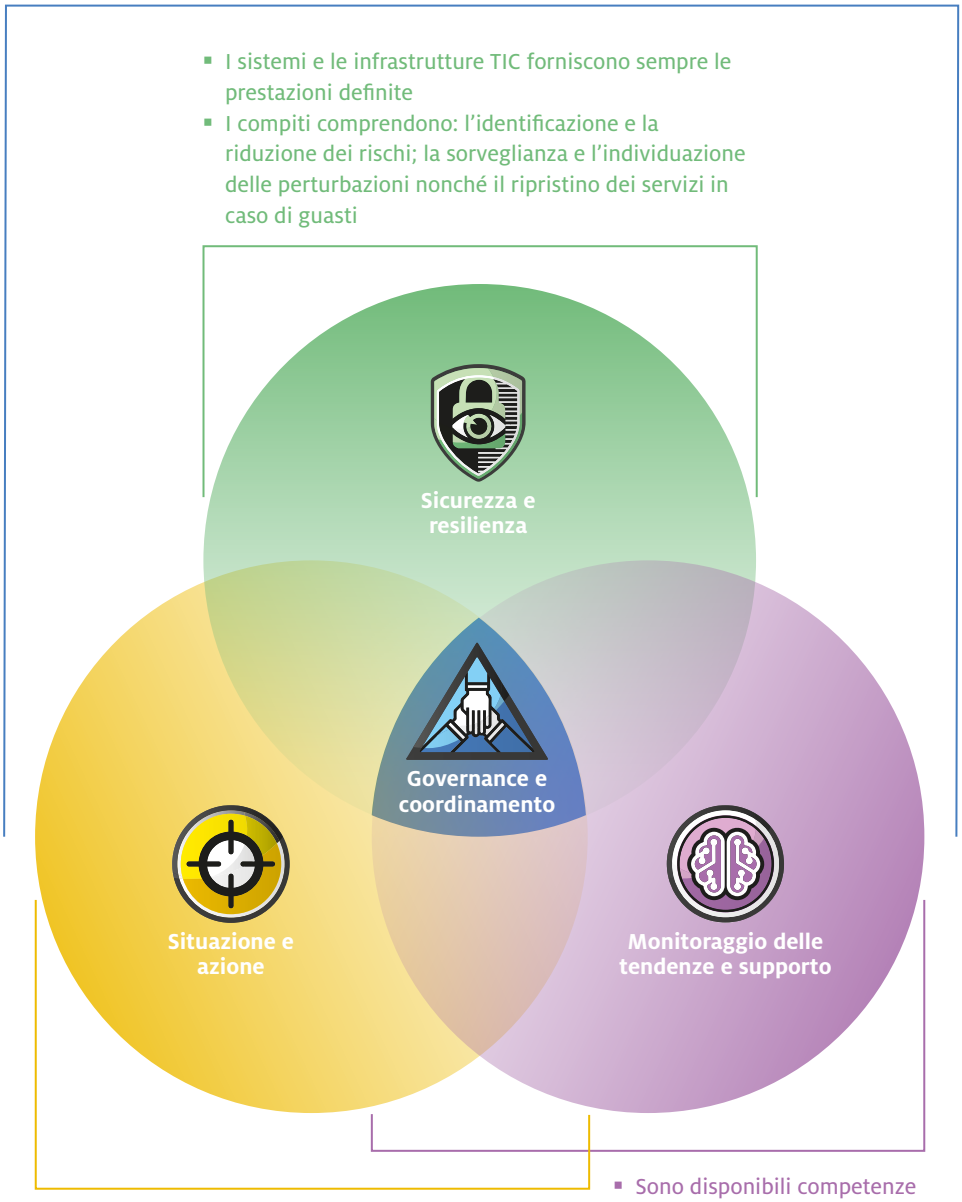
Resistenza: *quando sono presenti molte misure di protezione e il minor numero possibile di punti deboli, e la protezione può essere garantita a lungo.*

2 Occorre tra l'altro adottare misure preventive nei settori della tecnologia, dei processi e del personale.

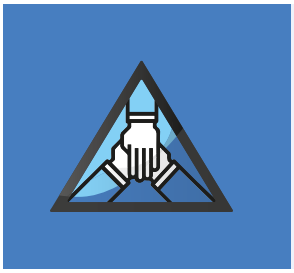
Ciberdifesa DDPS: quattro settori principali

La Strategia Ciber DDPS suddivide le misure da adottare in quattro settori tematici. Questi comprendono: la situazione e l'azione; la sicurezza e la resilienza; il monitoraggio delle tendenze e il supporto. La governance e il coordinamento costituiscono il quarto elemento connettivo. Ogni settore dipartimentale suddivide anch'esso le proprie azioni in questi ambiti tematici.

- Creare le premesse per lo sviluppo e l'uso di tutte le risorse necessarie
- Sorvegliare il progresso dell'attuazione e coordinare la collaborazione con le parti coinvolte



Settori fondamentali e compiti del DDPS



Governance e coordinamento
Al livello strategico di ogni unità amministrativa (UA) del DDPS vengono create le premesse per lo sviluppo e l'uso di tutte le risorse necessarie. Il progresso dell'attuazione viene sorvegliato e la collaborazione con le parti coinvolte coordinata.
Esempio: *sviluppo dell'organizzazione: i settori dipartimentali stilano un'analisi delle sfide nel ciberspazio e una panoramica dei relativi livelli; laddove necessario, hanno luogo decisioni e sviluppi tempestivi sulla base delle analisi.*

Sicurezza e resilienza
Questo settore fondamentale struttura i compiti, affinché tutti i sistemi e le infrastrutture TIC siano organizzati e gestiti in modo tale da poter fornire le prestazioni definite. In tal modo si vuole ottenere che le UA del DDPS possano adempiere i loro compiti in ogni momento e in tutte le situazioni. Tali compiti spaziano dall'identificazione alla riduzione dei rischi passando per la sorveglianza e l'individuazione delle perturbazioni fino al ripristino dei servizi.
Esempio: *sviluppare misure volte a ripristinare sistemi dopo un incidente.*

Situazione e azione
Questo settore fondamentale comprende tutti i compiti necessari all'anticipazione, all'individuazione precoce, alla prevenzione e all'attribuzione di ciberattacchi rilevanti sul piano della politica di sicurezza. Comprende anche la valutazione della minaccia e la rappresentazione della situazione. A ciò si aggiungono l'acquisizione di informazioni di intelligence e lo svolgimento di ciberoperazioni (contromisure nel quadro della ciberdifesa nonché gli effetti attivi nel ciberspazio in situazioni simili a quelle che si registrano in caso di conflitto).
Esempio: *potere adottare cibercontromisure difensive in caso di attacco.*

Monitoraggio delle tendenze e supporto
Le competenze chiave necessarie per lo sviluppo dei mezzi tecnici, specialistici e personali delle UA del DDPS vengono ampliate e messe a disposizione. Lo sviluppo e il trasferimento di conoscenze hanno luogo in collaborazione con le scuole universitarie e l'industria.
Esempio: *ricerca, sviluppo e innovazione: essere aggiornati sul piano tecnico, specialistico e del personale.*

Principi d'azione

Il rafforzamento della cibersicurezza della Svizzera è una priorità del DDPS. Per l'attuazione della strategia sono perciò stati formulati i seguenti principi d'azione:

Sussidiarietà: le cibercompetenze disponibili nel DDPS possono essere impiegate per appoggiare gli attori civili in caso di eventi, se le disposizioni legali sono soddisfatte. A tale scopo bisogna esercitare e intensificare la collaborazione, per esempio mediante il trasferimento di conoscenze ed esercitazioni.

Collaborazione istituzionale: il DDPS contribuisce con i suoi mezzi alla collaborazione con altri partner della politica di sicurezza in Svizzera. La collaborazione ha luogo con Cantoni, Comuni, partner in campo economico, sociale e scientifico nonché con partner internazionali. È disciplinata nell'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (OCiber).[3] Il delegato alla cibersicurezza della Confederazione coordina i tre settori seguenti: cibersicurezza, perseguimento penale della cibercriminalità e ciberdifesa (secondo la Strategia nazionale per la protezione della Svizzera contro i ciber-rischi SNPC).

Collaborazione internazionale: essa avviene a livello bilaterale e multilaterale con altri uffici della Confederazione (Dipartimento federale degli affari esteri, Dipartimento federale delle finanze, Dipartimento federale di giustizia e polizia) e serve soprattutto all'anticipazione e all'individuazione precoce di minacce e sfide nel ciberspazio.

Apertura / trasparenza: il DDPS coadiuva altri partner con le sue competenze.

Comando Ciber dell'esercito: conformemente al mandato del Consiglio federale, l'attuale Base d'aiuto alla condotta dell'esercito (BAC) sarà trasformata dall'inizio del 2024 in un Comando Ciber; la capacità d'impiego dell'esercito nel ciberspazio deve essere migliorata in permanenza.

La Strategia Ciber DDPS serve a garantire la migliore protezione possibile della Svizzera nel ciberspazio. Questa protezione viene garantita congiuntamente con i partner e serve a minimizzare la vulnerabilità della Svizzera nel ciberspazio.

Grazie alla collaborazione permanente dei partner interni ed esterni del DDPS nella quotidianità, gli eventi o le crisi possono essere gestite in modo più efficiente. I diversi processi sono rodati, i compiti sono conosciuti e la rete è collaudata. In tal modo la Strategia DDPS, mediante una pianificazione concreta delle misure, non garantisce solo un'attuazione professionale, ma rafforza anche i preparativi congiunti in vista del caso reale e la relativa gestione nella ciber-rete integrata.

---

3 RS 120.73 – Ordinanza del 27 maggio 2020 sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber) (admin.ch)

Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS
Segreteria generale SG-DDPS
Digitalizzazione e cibersicurezza DDPS (DCS DDPS)
Maulbeerstrasse 9, 3003 Berna

Premedia
Centro dei media elettronici CME
80.256.01 i 03.2021

I punti principali della Strategia Ciber DDPS

- Il DDPS è in grado permanentemente di gestire diverse minacce, eventi e crisi nel ciberspazio o di fornire supporto.
- Tutti gli attori con compiti rilevanti in ambito ciber nel DDPS si coordinano attivamente nel quadro della Strategia Ciber DDPS.
- I partner responsabili in seno al DDPS lavorano insieme per identificare rischi e opportunità oggi e in futuro ed essere pronti a gestirli congiuntamente.
- Il DDPS orienta il suo sviluppo sul piano specialistico, materiale, processuale come pure del personale in funzione delle cibersfide. In questo contesto rivestono un'importanza fondamentale l'istruzione e il perfezionamento di tutte le collaboratrici e di tutti i collaboratori del DDPS nonché dei militari (personale di professione e di milizia).
- I responsabili dell'ambito ciber in seno al DDPS collaborano con i partner. Questi sono i Cantoni e i Comuni, la ricerca e l'economia privata e anche il contesto internazionale. Il DDPS collabora a stretto contatto con il Centro nazionale per la cibersicurezza.