Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della protezione della popolazione UFPP

Stato febbraio 2023 *)

Strategie nazionali Protezione delle infrastrutture critiche PIC / Cyber SNPC

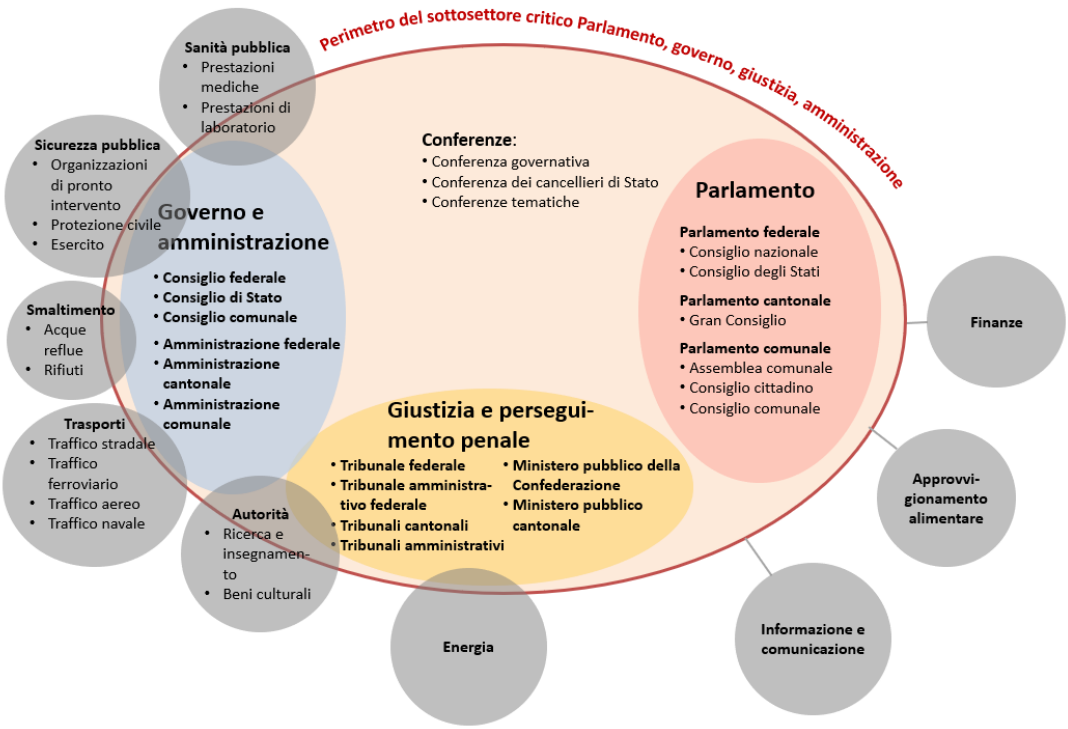
Factsheet sul sottosettore critico Parlamento, governo, giustizia, amministrazione

Descrizione generale e prestazioni del sottosettore

Il sottosettore Parlamento, governo, giustizia, amministrazione eroga numerose prestazioni importanti per la popolazione e l'economia. Vi rientrano la legislazione, la giurisdizione e la loro esecuzione, nonché servizi amministrativi statali, come il rilascio di permessi e il loro controllo. Per la maggior parte di queste prestazioni, perturbazioni di breve durata o interruzioni di poche ore o giorni non cagionano gravi danni per la popolazione e l'economia.

Critici in termini di tempo sono soprattutto i processi per le operazioni di sdoganamento nell'ambito del commercio internazionale, la gestione di elenchi e registri frequentemente utilizzati (banche dati della polizia, registri fondiari, registri elettorali, ecc.) e la protezione della popolazione in caso di pericolo (informazione, allerta o allarme alla popolazione).

Le autorità erogano prestazioni rilevanti anche per tutti gli altri settori critici. I compiti che concernono direttamente altri sottosettori, ad esempio l'attività di vigilanza degli impianti d'accumulazione nel sottosettore dell'approvvigionamento energetico, sono però analizzati direttamente nel factsheet corrispondente.



Analisi del mercato / Struttura del sistema

Il sottosettore Parlamento, governo, giustizia e amministrazione ha una struttura decentralizzata con gli ambiti Esecutivo, Legislativo e Giudiziario e i tre livelli Confederazione, Cantoni e Comuni. All'interno di questi ambiti, il sottosettore è composto da singoli attori rilevanti per il sistema che assumono compiti specifici nella loro sfera di competenza. Questi attori possono sostenersi a vicenda solo in misura limitata. Le conseguenze delle interruzioni sono però spazialmente circoscritte e, poiché molti compiti possono essere posticipati, non sono solitamente critiche in termini di tempo.

*) I contenuti del presente factsheet si basano sull'analisi dei rischi e delle vulnerabilità dell'UFPP del 2018.

Processi esaminati

Nell'ambito dell'analisi dei rischi e delle vulnerabilità sono stati esaminati più in dettaglio 13 processi che sono importanti per la funzionalità delle autorità o che assumono una grande importanza già a breve termine per la popolazione e l'economia:

Parlamento (legislativo)	**Governo e amministrazione (esecutivo)**	**Giustizia (giudiziario)**
Processi chiave	***Processi chiave***	***Processi chiave***
– Emanazione di leggi – Processo decisionale parlamentare	– Servizi amministrativi generali – Compiti di salvaguardia della sicurezza interna – Gestione di elenchi e registri – Protezione della popolazione, dell'economia e dell'ambiente in caso di pericolo – Garanzia dei diritti politici – Operazioni di sdoganamento	– Giurisprudenza – Perseguimento penale
Processi di supporto	***Processi di supporto***	***Processi di supporto***
– Prestazioni di supporto dei servizi del Parlamento	– Mantenimento dell'infrastruttura, incl. sistemi TIC	– Prestazioni di supporto dei servizi di tribunale

Pericoli rilevanti per il sottosettore critico

Cyberattacco

Blackout

Interruzione TIC

Attentato convenzionale

Nota: i pericoli esaminati sono rilevanti per l'intero sottosettore. Per certe aziende/infrastrutture critiche, possono essere rilevanti anche altri rischi.

Vulnerabilità e rischi

Le maggiori vulnerabilità dei processi esaminati concernono i sistemi TIC utilizzati in condivisione da Confederazione, Cantoni e Comuni. Questi dipendono fortemente dal funzionamento delle reti di telecomunicazione pubbliche e dall'alimentazione elettrica. Nell'ambito dell'analisi dei rischi, sono stati esaminati vari scenari, come cyberattacchi ai sistemi TIC delle autorità (p.es banche dati e registri), un blackout sovraregionale, un guasto presso un fornitore centrale di servizi TIC e un attentato a un'importante infrastruttura delle autorità.

L'analisi evidenzia che simili eventi causano danni economici e sociali diretti, ad esempio l'impossibilità di svolgere numerosi compiti senza estratti di registro. Anche i danni secondari indiretti di tali eventi possono essere gravi. Interruzioni di lunga durata dei sistemi o delle infrastrutture statali potrebbero minare la fiducia della popolazione nelle autorità e danneggiare la reputazione della Svizzera (con conseguenze per la piazza economica e il turismo).

Nel complesso, il sottosettore Parlamento, governo, giustizia e amministrazione può essere considerato relativamente resiliente. Sono in corso di pianificazione o realizzazione vari progetti e programmi nel campo dell'approvvigionamento elettrico e della resilienza delle TIC, che contribuiranno a rafforzare ulteriormente questa resilienza. Ne sono un esempio il Raggruppamento dei centri di elaborazione dati o la Rete di dati sicura (RDS). In futuro si prevede però che in mancanza di misure d'accompagnamento l'attuale resilienza del sottosettore diminuirà a causa della progressiva interconnessione dei sistemi TIC.

Misure di resilienza

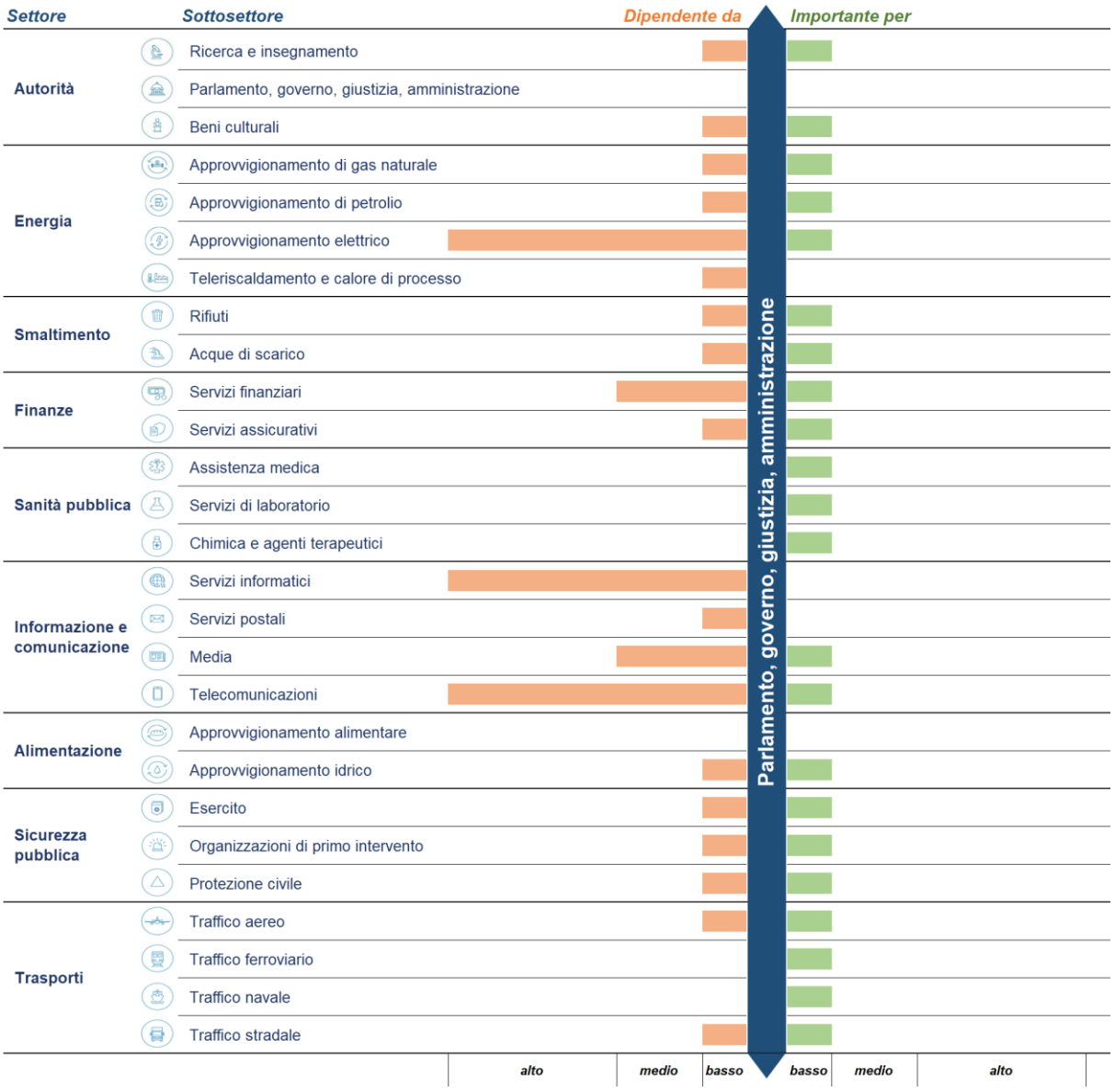
Migliorare lo scambio di informazioni

- Intensificare la collaborazione tra tutti i livelli (Confederazione, Cantoni e Comuni) nel campo dei cyber-rischi e delle dipendenze TIC

Comunicazione in caso d'evento

- Valutare le ridondanze nel campo della comunicazione con le rappresentanze svizzere all'estero
- Verificare l'informazione e la comunicazione durante gli eventi
- Valutare l'utilizzo o l'allacciamento alla Rete di dati sicura (RDS)

Interdipendenze del sottosettore Parlamento, governo, giustizia, amministrazione



Maggiori informazioni online sulla PIC e sulla SNPC

www.infraprotection.ch

www.ncsc.admin.ch