



Corso di formazione cyber



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Esercito svizzero

Il corso di formazione cyber dell'Esercito svizzero

- L'esercito deve poter proteggere i propri sistemi d'informazione e di comunicazione nonché respingere cyberattacchi in ogni momento, nella normale quotidianità come pure in caso di crisi.
- A tale scopo impiega parti dell'organizzazione di professionisti della Base d'aiuto alla condotta (BAC), che vengono appoggiate da militari di milizia dell'esercito.
- Con l'ulteriore sviluppo dell'esercito (USEs) è stata creata una compagnia cyber nel Gruppo elettronica 46 (gr elo 46) in seno alla brigata d'aiuto alla condotta 41 (br aiuto cond 41/SIS). Il compito di questa compagnia consiste nel fornire appoggio all'organizzazione di professionisti della BAC. Il corso di formazione cyber ha lo scopo di istruire i futuri militi della compagnia cyber.
- Il corso di formazione cyber si svolge due volte all'anno. L'obiettivo è quello di istruire circa dodici reclute per ogni corso.
- Il corso di formazione cyber dura 40 settimane, si svolge presso la scuola della guerra elettronica 64 (scuola GE 64) e comprende 800 ore d'istruzione e d'impiego in ambito cyber.
- Al termine del corso di formazione è possibile assolvere un esame che permette di ottenere un attestato professionale federale.

Selezione

- **Specialisti** con apprendistato completato di informatico/a AFC, mediamatico/a AFC, operatore/trice informatico/a AFC.
- **Liceali** con approfondimento in materie scientifiche.
- **Studenti** in informatica, fisica, matematica, elettrotecnica, automazione e/o pedagogia.
- **Persone autodidatte** che hanno acquisito conoscenze approfondite nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) / cyber.
- Disponibilità all'avanzamento a **sergente**.
- **Personalità adeguata:** capacità di apprendimento superiore alla media, resistenza allo stress, discrezione, senso di responsabilità.
- Elevata **motivazione** ad affrontare contenuti impegnativi.
- Controllo di sicurezza relativo alle persone ampliato superato.
- Lingue: inglese nonché tedesco oppure francese, con buone conoscenze passive di una seconda lingua nazionale.

1. Obiettivi

L'esercito deve poter proteggere i propri sistemi d'informazione e di comunicazione nonché respingere cyberattacchi in ogni momento, nella normale quotidianità come pure in caso di crisi. Impiega i mezzi pertinenti in modo da poter proteggere sé stesso e adempiere il suo mandato.

Dal 2018 l'Esercito svizzero organizza il corso di formazione di base cyber destinato ai militari di milizia dell'Esercito svizzero. Grazie a questo corso di formazione, le cittadine e i cittadini svizzeri abili al servizio militare hanno la possibilità di prestare il servizio militare nell'impegnativo ambito cyber dell'esercito già a partire dall'inizio della scuola reclute. La milizia appoggia le organizzazioni di professionisti nell'autoprotezione dei sistemi d'informazione e delle reti informatiche militari, garantisce la capacità di resistenza a livello di personale e completa le competenze specifiche mancanti o insufficienti.

Dopo aver concluso con successo il corso di formazione i militari sono incorporati nel gr elo 46 in seno alla br aiuto cond 41/SIS. L'impiego nei corsi di ripetizione ha lo scopo di sorvegliare e proteggere le infrastrutture e i sistemi informatici e di comunicazione dell'Esercito svizzero. L'organizzazione di professionisti della Base d'aiuto alla condotta, responsabile di tale ambito, integra i militari nelle attività quotidiane e li accompagna sul piano specialistico.

2. Organizzazione

Il corso di formazione si svolge due volte all'anno presso la scuola GE 64 a Jassbach, nel quadro della SR GE 64. La scuola GE 64 è responsabile della condotta e dell'istruzione militare, mentre l'istruzione specialistica in ambito cyber è garantita dall'organizzazione di professionisti della BAC.

3. Contenuto e struttura

Le persone che concludono con successo il corso di formazione dispongono delle conoscenze e delle capacità necessarie per adempiere il proprio compito militare in uno dei tre settori specialistici seguenti.

Impiego nel quadro delle **Computer Network Operations** (CNO), per esempio in veste di:

- sviluppatore di strumenti software;
- analista di avvenimenti e attacchi cyber;
- analista di vulnerabilità informatiche.

Impiego nel quadro del **Cyber Fusion Center** (CFC), per esempio con i seguenti compiti:

- analisi di cyberminacce rivolte contro i sistemi d'informazione del DDPS e dell'esercito;
- indagini tecniche su sistemi, componenti hardware e apparecchi mobili;
- analista in un Security Operation Center (SOC).

Impiego nel quadro della **Cyber Defence** (CYD), per esempio con i seguenti compiti:

- redazione di contributi parziali sulla situazione cyber dell'Esercito svizzero;
- appoggio, consulenza e istruzione in ambito cyber a favore di militari di altre Armi;
- redazione di contributi nel campo del servizio informazioni.

| Modulo | Materia | Ore | Luogo |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------|
| Basi generali <i>TUTTI I PARTECIPANTI</i> | <ul style="list-style-type: none">• Compiti, organizzazione e mezzi dell'esercito• Compiti, organizzazione e mezzi della Base d'aiuto alla condotta• Etica e responsabilità individuale• Basi legali | 60 | Jassbach |
| Basi tecniche <i>TUTTI I PARTECIPANTI</i> | <ul style="list-style-type: none">• Approfondimento delle basi TIC• Corso di base crittologia• Cybersicurezza applicata | 170 | Jassbach |
| Istruzione trasversale <i>TUTTI I PARTECIPANTI</i> | <ul style="list-style-type: none">• Armonizzazione delle conoscenze CFC, Cyber Defence e CNO | 30 | Jassbach |
| Formazione alla condotta (secondo criteri ASFC) <i>TUTTI I PARTECIPANTI</i> | <ul style="list-style-type: none">• Modulo Leadership• Modulo Comunicazione• Modulo Gestione dei conflitti• Modulo Conoscenza di sé• Modulo Metodica dell'istruzione | 90 | Jassbach |
| Istruzione specialistica <i>IN BASE ALLA FUNZIONE (CNO/ CFC/CYBER DEFENCE)</i> | <ul style="list-style-type: none">• Istruzione specialistica approfondita in vista della futura funzione militare (classificata). | 300 | Jassbach e regione di Berna |
| Impiego ed esercizi <i>TUTTI I PARTECIPANTI NEI RISPETTIVI AMBITI SPECIALISTICI, IN PARTE INSIEME</i> | <ul style="list-style-type: none">• Esercizi militari specifici in collaborazione con ambiti specialistici BAC e gestori TIC di altre scuole reclute.• Esercizi militari specifici in collaborazione con ambiti specialistici BAC e gestori TIC di altre scuole reclute. | 150 | Jassbach e regione di Berna |
| Totale ore d'istruzione | | 800 | |

4. Svolgimento del corso di formazione

La vasta materia d'insegnamento non può essere trattata in una scuola reclute di 18 settimane. Per tale motivo viene sempre svolta l'istruzione di 40 settimane fino al grado di sergente e la disponibilità all'avanzamento rappresenta quindi un presupposto irrinunciabile.

| Corso di formazione cyber (40 settimane) | | | | | | | |
|------------------------------------------|-------------|-------------|-------------|--------------------------------|-------------|-------------|--------------------------------|
| SR GE 64-1 | | | SSU GE | SR GE 64-2 | | | |
| IBG * | IBF | IDR | SSU | Servizio pratico come sergente | | | |
| 6 settimane | 7 settimane | 5 settimane | 4 settimane | 18 settimane | | | |
| Corso di formazione successivo | | | IBG * | IBF | IDR | SSU | Servizio pratico come sergente |
| | | | 6 settimane | 7 settimane | 5 settimane | 4 settimane | 18 settimane |

Sulla base delle necessità specifiche del corso di formazione, alcune fasi d'istruzione potrebbero essere adeguate. A differenza delle altre Armi non viene svolta l'abituale istruzione di reparto, in quanto l'impiego non si svolge nel quadro di reparti (gruppi, sezioni o compagnie) bensì con distaccamenti organizzati in funzione del compito.

La tabella seguente illustra la suddivisione della materia d'insegnamento cyber nelle abituali fasi dell'istruzione a sergente.

| Fase dell'istruzione | Materia / impiego |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Istruzione di base generale (IBG) | <ul style="list-style-type: none"> Modulo «Basi generali» |
| Istruzione di base alla funzione (IBF) | <ul style="list-style-type: none"> Modulo «Basi tecniche» Modulo «Istruzione trasversale» Parti del modulo «Istruzione specialistica» |
| Istruzione di reparto (IDR) | <ul style="list-style-type: none"> Parti del modulo «Istruzione specialistica» Impiego nel quadro dell'organizzazione di professionisti BAC |
| Scuola sottufficiali (SSU) | <ul style="list-style-type: none"> Modulo «Formazione alla condotta» |
| Servizio pratico | <ul style="list-style-type: none"> Conclusione del modulo «Formazione alla condotta» Impiego nel quadro dell'organizzazione di professionisti BAC Impiego quale capogruppo e istruttore |

Durante il servizio pratico come sergente sono previste le seguenti attività:

- impiego quale capogruppo e istruttore a livello di gruppo;
- istruttore per lezioni specialistiche in ambito cyber;
- impiego nel quadro dell'organizzazione di professionisti BAC nel proprio settore specialistico;
- allenamento «on the job» sui sistemi d'impiego da parte dell'organizzazione di professionisti BAC;
- condotta di team e gruppi in impiego, 24 ore su 24 per la durata di giorni – settimane.

* L'IBG viene conclusa nella scuola in cui si è stati chiamati in servizio per la SR. Il passaggio alla SR GE 64 e al corso di formazione cyber avviene alla fine dell'IBG (dopo aver superato la selezione).

5. Istruzione

Per poter raggiungere gli impegnativi obiettivi didattici, durante il corso di formazione vengono combinati svariati metodi d'insegnamento:

- lezione frontale classica seguita da esercizi per consolidare la materia;
- elaborazione autonoma di contenuti, per es. sulla base della bibliografia o con ricerche online;
- acquisizione autonoma di competenze risolvendo in modo pratico dei problemi con un sistema d'allenamento cyber;
- applicazione e approfondimento della materia acquisita con esercizi in un «Cyber Training Range»¹, in cui è possibile simulare in modo diretto cyberattacchi ad alta intensità;
- impiego nel quadro di compiti reali dell'organizzazione di professionisti della BAC. In quest'ambito i partecipanti vengono seguiti, valutati, istruiti e stimolati in modo intenso e continuo dagli specialisti della BAC.

Per garantire che la materia insegnata sia attuale e affinché sia possibile mantenere uno stretto contatto con gli istituti di formazione in Svizzera, viene attribuita particolare attenzione al corpo docenti. I contenuti militari e rilevanti ai fini dell'impiego vengono trattati da specialisti della BAC con vasta esperienza. Le basi tecniche generali in ambito cyber sono trattate da insegnanti esterni con un mandato d'insegnamento presso una scuola universitaria oppure con comprovate competenze didattiche e specialistiche.

6. Possibilità di carriera militare

Il corso di formazione cyber è in larga misura orientato agli abituali criteri d'istruzione dell'esercito; per i partecipanti è quindi senz'altro possibile un avanzamento militare a ufficiale, sia diventando comandante di compagnia e in seguito ufficiale di stato maggiore generale sia per seguire la carriera di ufficiale di stato maggiore.

7. Assessment e selezione continua

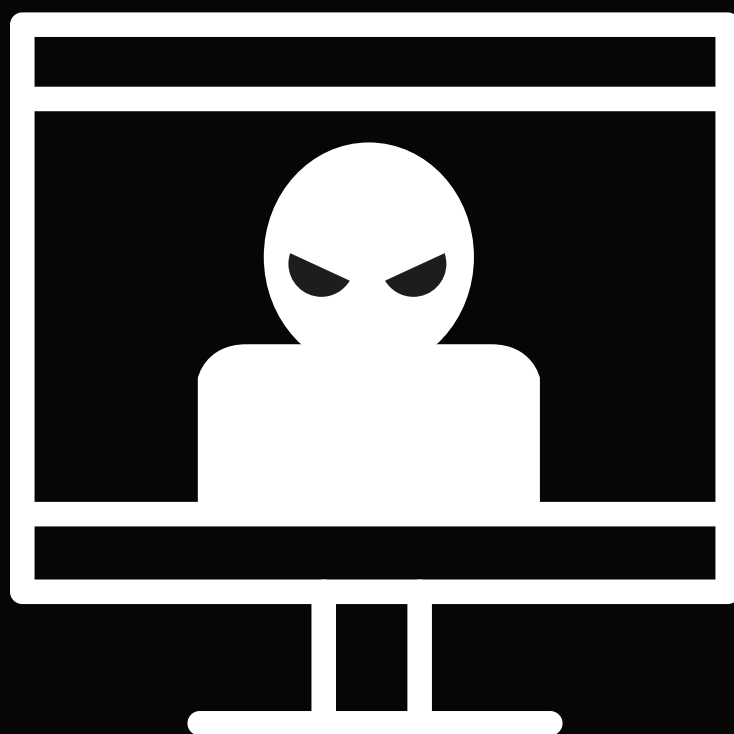
Indipendentemente dalla precedente formazione civile, i partecipanti vengono ammessi definitivamente solo dopo aver superato un assessment svolto dall'organizzazione di professionisti della BAC all'inizio della scuola reclute. I partecipanti che durante il corso di formazione forniscono prestazioni insufficienti vengono trasferiti in un pool provvisorio. In assenza di un miglioramento delle prestazioni i partecipanti vengono assegnati a un'altra funzione all'interno dell'ambito GE.

8. Certificati

- Al termine del corso di formazione è possibile assolvere l'esame di «Cyber Security Specialist» con attestato professionale federale.
- La scuola universitaria professionale di Lucerna computa 21 punti ECTS agli studenti provenienti dal corso di formazione cyber che intendono iscriversi al ciclo di studi bachelor «Information- and Cyber-Security». Il riconoscimento del corso di formazione presso altri istituti accademici è attualmente in fase di accertamento.
- Anche la formazione alla condotta svolta con l'avanzamento a sergente può essere conclusa con un attestato riconosciuto in ambito civile.
Ulteriori informazioni sono disponibili al sito www.vtg.admin.ch/it/organizzazione/kdo-ausb/hka/zs/cfoc.html.
- Anche i candidati che non assolvono o non superano gli esami citati vengono incorporati nel gr elo 46.



¹ Il «Cyber Training Range» è un sistema d'istruzione autonomo che permette di trattare nella pratica argomenti cyber. Il sistema è fisicamente separato dai sistemi produttivi «reali» della BAC.



Fighting
hackers.

Contatto

Esercito svizzero
Base d'aiuto alla condotta
cyber.fub@vtg.admin.ch
www.cyberdefence.ch