

# Profilo di qualificazione per la professione di Cyber Security Specialist con brevetto federale

Versione 1.1 del 27.02.2019

## Indice

1	Introduzione .....	2
2	Profilo della professione.....	3
2.1	Campo d'attività .....	3
2.2	Principali competenze operative.....	3
2.3	Esercizio della professione .....	3
2.4	Importanza della professione per la società, l'economia, la natura e la cultura .....	3
3	Competenze operative e criteri di prestazione.....	4
3.1	Tabella delle competenze operative .....	4
3.2	CCO A: protezione preventiva dei sistemi.....	5
3.3	CCO B: Identificazione di incidenti concernenti la sicurezza.....	7
3.4	CCO C: gestione degli incidenti concernenti la sicurezza .....	9
3.5	CCO D: pianificazione e attuazione di soluzioni concernenti la sicurezza.....	11



## **1 Introduzione**

Il presente profilo di qualificazione per la professione di Cyber Security Specialist con brevetto federale è stato elaborato su mandato di ICT-Formazione professionale Svizzera da un gruppo di lavoro costituito da rappresentanti del mondo economico e dell'amministrazione, sotto la guida di eduxept AG.

Il documento descrive il profilo della professione, le competenze operative e il profilo dei requisiti mediante criteri per la valutazione delle prestazioni. Queste basi servono all'elaborazione del regolamento d'esame, delle direttive sul regolamento d'esame e delle descrizioni dei moduli per il piano modulare.

Il documento è stato approvato nell'ambito di una procedura di deliberazione per mezzo di circolare l'8 ottobre 2018 dal comitato di coordinamento del progetto e il 23 ottobre 2018 dalla Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI).

## **2 Profilo della professione**

### **2.1 Campo d'attività**

I Cyber Security Specialist (CSS) costituiscono una manodopera altamente specializzata attiva nel campo della cybersicurezza. Essi operano generalmente all'interno di medie o grandi imprese private o presso istituzioni pubbliche. I loro compiti principali consistono nella protezione preventiva dei sistemi d'informazione e di comunicazione di un'organizzazione contro gli attacchi nel cyberspazio e nella gestione reattiva degli incidenti in ambito di sicurezza.

I Cyber Security Specialist possono dirigere piccoli team costituiti da professionisti incaricati della gestione operativa o impegnati in progetti specifici. Nell'ambito dei progetti, essi si assumono la responsabilità per lavori individuali o sotto-progetti.

### **2.2 Principali competenze operative**

I Cyber Security Specialist

- analizzano costantemente le attuali cyberminacce e anticipano le minacce rilevanti per la loro organizzazione;
- contollano la sicurezza dei sistemi, identificano i punti vulnerabili e adottano misure di protezione preventiva per porvi rimedio;
- sorvegliano i sistemi in funzione e individuano gli incidenti concernenti la sicurezza e le non conformità rispetto alle direttive sulla sicurezza di un'organizzazione;
- analizzano le cause e le ripercussioni degli incidenti concernenti la sicurezza e rispondono con misure di protezione reattive;
- pianificano progetti nel campo della cybersicurezza e li concretizzano;
- consigliano e formano sul piano tecnico i target interessati.

### **2.3 Esercizio della professione**

La cybersicurezza costituisce un campo d'attività specifico della gestione delle tecnologie dell'informazione e della comunicazione (ICT). L'integrazione della cybersicurezza nell'organizzazione funzionale e strutturale di un'impresa o di un'amministrazione varia in funzione della dimensione e dell'orientamento di quest'ultima. Generalmente, i Cyber Security Specialist collaborano con altri specialisti della sicurezza ICT di un'organizzazione (Security Operations Center [SOC]). Le procedure e le regole della strategia di sicurezza del management e le relative direttive sulla sicurezza (politica di sicurezza dell'informazione) formano il contesto di lavoro dei Cyber Security Specialist.

Oltre a solide conoscenze tecniche, l'esercizio della professione di Cyber Security Specialist richiede una grande vivacità di spirito, una capacità di riflessione analitica e sistemica sviluppata, la capacità di ragionare in termini di processi, il senso di responsabilità, la tolleranza alla frustrazione, la facilità di comunicazione e un ottimo spirito di squadra senza dimenticare discrezione, integrità e perseveranza.

### **2.4 Importanza della professione per la società, l'economia, la natura e la cultura**

L'utilizzo delle tecnologie dell'informazione e della comunicazione aumenta in tutti i contesti della vita. La crescente importanza dell'informazione e della tecnologia sta inoltre aumentando il rischio di abusi con un significativo potenziale di danno per l'economia e la società. I Cyber Security Specialist contribuiscono a proteggere i sistemi, le applicazioni e i dati contro gli utilizzi illeciti delle tecnologie e, pertanto, a minimizzare i danni patrimoniali e materiali, i pregiudizi verso le persone e il sapere. Essi contribuiscono inoltre all'immagine della Svizzera in quanto piazza economica sicura e partner politico e commerciale affidabile.

### 3 Competenze operative e criteri di prestazione

#### 3.1 Tabella delle competenze operative

↓ Campi di competenze operative CCO      Competenze operative →

<b>A</b>	<b>Protezione preventiva dei sistemi</b>	A1: seguire costantemente l'evoluzione delle minacce	A2: analizzare le minacce e trattare le informazioni	A3: individuare i punti vulnerabili	A4: porre rimedio ai punti vulnerabili	A5: utilizzare procedure ingannevoli	A6: fornire consulenze tecniche agli stakeholder	A7: formare gli stakeholder
<b>B</b>	<b>Identificazione di incidenti concernenti la sicurezza</b>	B1: controllare i sistemi di monitoraggio in funzione	B2: analizzare e interpretare dati	B3: selezionare gli incidenti concernenti la sicurezza	B4: documentare gli incidenti concernenti la sicurezza	B5: sorvegliare il trattamento di un incidente concernente la sicurezza		
<b>C</b>	<b>Gestione degli incidenti concernenti la sicurezza</b>	C1: attuare misure immediate	C2: assicurare la conservazione delle prove	C3: analizzare le cause e le ripercussioni	C4: definire e attuare misure di protezione	C5: sostenere il ripristino dei sistemi		
<b>D</b>	<b>Pianificazione e attuazione di soluzioni concernenti la sicurezza</b>	D1: delimitare i sistemi e specificare le esigenze	D2: verificare l'affidabilità e l'efficienza	D3: determinare l'investimento in risorse e inserirlo nel budget	D4: procedere a una valutazione	D5: attuare un progetto	D6: dirigere un team	

### 3.2 CCO A: protezione preventiva dei sistemi

Descrizione del campo di competenze operative (CCO)		
<p>Il CCO A include le competenze operative esercitate dai Cyber Security Specialist (CSS) nei settori <b>Anticipazione</b> e <b>Prevenzione</b>. Le attività che rientrano in questi campi riguardano l'individuazione precoce delle potenziali minacce e la riduzione delle possibilità di attacchi mediante l'adozione di misure di protezione preventive.</p> <p>Basandosi su varie fonti d'informazione e sugli scambi di esperienze, i CSS seguono e analizzano costantemente l'evoluzione attuale delle minacce da cui traggono delle costatazioni e delle informazioni a livello tattico, operativo e tecnico, da elaborare all'attenzione delle autorità decisionali.</p> <p>Attraverso procedure e strumenti selezionati, i CSS individuano i punti vulnerabili delle reti, delle applicazioni e delle soluzioni di stoccaggio nonché degli apparecchi terminali e periferici. Per determinare se bisogna porre rimedio a una situazione vulnerabile, i CSS tengono conto del rapporto costi/benefici, nonché delle direttive e dei processi dell'organizzazione. Se necessario, i CSS utilizzano delle procedure tecniche e degli strumenti per ingannare gli aggressori.</p> <p>I CSS formano e consigliano le varie parti interessate sugli aspetti tecnici contribuendo così a sensibilizzarle sulla cybersicurezza, ciò che costituisce un elemento essenziale di una prevenzione efficace.</p>		
Contesto		
<p>La portata e la natura della prevenzione sono determinate in larga misura dalla propensione al rischio e dalla valutazione del rischio del management. Le misure preventive sono efficaci ed economiche se conformi alla gestione dei rischi definita nella strategia di sicurezza globale.</p> <p>L'utilizzo di procedure e di strumenti per l'individuazione dei punti deboli deve tener conto delle disposizioni del diritto penale (ad esempio il furto di dati, intrusione non autorizzata in un sistema informatico) e della protezione dei dati.</p> <p>Le minacce e gli scenari di attacchi evolvono e cambiano in modo estremamente dinamico nel cyberspazio. Oltre a competenze personali decisive, l'acquisizione effettiva di informazioni e di conoscenze richiede anche una solida rete di relazioni e di comunicazione con i vari partner rilevanti.</p> <p>Relazione con il campo di competenze D: nei campi Anticipazione e Prevenzione, possono verificarsi nella pratica dei bisogni di soluzioni di sicurezza più estesi o più complessi. Questi bisogni sono generalmente trattati nell'ambito di progetti specifici, al di fuori della gestione operativa normale. Le competenze operative dei CSS legate a progetti sono descritte nel campo di competenze D.</p>		
Competenza operativa	Precisazioni sul contenuto e terminologia specifica	Criteri di prestazione (CP)
A1: seguire costantemente l'evoluzione delle minacce	- Fonti d'informazione quali i cataloghi delle minacce MELANI, BSI, rapporti di sicurezza dei fabbricanti, forum, organi specializzati, ecc.	I CSS sono in grado: CP-A-1: di differenziare le varie fonti d'informazione sulle minacce
A2: analizzare le minacce e trattare le informazioni	- Concetto e livelli della Cyber Threat Intelligence (CTI) (strategico, tattica, operativo e tecnico)	CP-A-2: di valutare la credibilità delle fonti e delle informazioni
A3: identificare i punti vulnerabili	- Audit e tipi di audit (audit dei sistemi, audit dei processi, audit dell'efficienza e audit della conformità)	CP-A-3: di ampliare le loro conoscenze sulle minacce in maniera continua, proattiva e autonoma

	<ul style="list-style-type: none"> <li>- Procedure e strumenti per i test di penetrazione, i Vulnerability-Scans e i Compliance-Scans</li> <li>- Indicators of Compromise (IoC) e Indicators of Attack (IoA)</li> <li>- Threat hunting proattivo</li> <li>- Quadro legale in materia di pirateria informatica</li> </ul>	<p>CP-A-4: di spiegare il concetto di Cyber Threat Intelligence</p> <p>CP-A-5: di identificare la rilevanza delle minacce per la loro organizzazione</p> <p>CP-A-6: di preparare, realizzare e valutare degli audit</p> <p>CP-A-7: di selezionare e utilizzare delle procedure e degli strumenti per identificare i punti vulnerabili in funzione del contesto e dei sistemi</p>
A4: porre rimedio ai punti vulnerabili	<ul style="list-style-type: none"> <li>- Direttive della strategia di sicurezza dell'informazione (polizia di sicurezza dell'informazione [PSI])</li> <li>- Misure di protezione tecniche e organizzative (MTO) specifiche ai sistemi, soluzioni di sicurezza e best practice</li> <li>- Metodi di inasprimento dei sistemi (hardening)</li> </ul>	<p>CP-A-8: di definire e attuare misure di protezione tecniche od organizzative appropriate</p> <p>CP-A-9: di selezionare ed utilizzare procedure e strumenti appropriati per ingannare gli aggressori</p>
A5: utilizzare procedure ingannevoli	<ul style="list-style-type: none"> <li>- Procedure e strumenti per ingannare gli aggressori (ad es. Honeypots, Traps, Decoys o strumenti che servono a mascherarsi)</li> </ul>	<p>CP-A-10: di valutare la conformità legale e normativa di tutte le misure prese nei settori Anticipazione e Prevenzione</p>
A6: fornire consulenze tecniche agli Stakeholder	<ul style="list-style-type: none"> <li>- Principi della consulenza sistemica orientata alle soluzioni</li> <li>- Modelli e regole di comunicazione</li> </ul>	<p>CP-A-11: di consigliare gli stakeholder sul piano tecnico secondo un approccio orientato ai bisogni e alle soluzioni</p>
A7: formare gli Stakeholder	<ul style="list-style-type: none"> <li>- Principi metodologici e didattici</li> <li>- Pianificazione e svolgimento di formazioni</li> </ul>	<p>CP-A-12: di elaborare dei contenuti specializzati in maniera metodologica e didattica</p>
<b>Competenze personali e sociali</b>		<p>CP-A-13: di pianificare, svolgere e valutare delle formazioni</p>
<ul style="list-style-type: none"> <li>- Curiosità e disponibilità ad imparare</li> <li>- Capacità di cambiare prospettiva (pensare come un aggressore)</li> <li>- Senso di responsabilità nell'utilizzo di procedure sensibili per individuare i punti vulnerabili o ingannare gli aggressori</li> <li>- Confidenzialità e integrità nel trattamento dei dati e delle informazioni sensibili</li> <li>- Facilità di comunicazione nell'ambito delle attività di consulenza e di formazione</li> </ul>		

### 3.3 CCO B: Identificazione di incidenti concernenti la sicurezza

Descrizione del campo di competenze operative (CCO)		
<p>Il CCO B include le competenze operative esercitate dai Cyber Security Specialists (CSS) nel settore <b>Identificazione</b>. Le attività che rientrano in questo campo concorrono all'identificazione degli incidenti concernenti la sicurezza nella gestione operativa.</p> <p>I CSS registrano mediante strumenti selezionati i dati pertinenti nelle reti, applicazioni e soluzioni di stoccaggio nonché in occasione dell'utilizzo di apparecchi terminali e periferici. I dati registrati sono oggetto di una valutazione e di un'analisi manuale o automatizzata in tempo reale o in differita per quanto riguarda le anomalie o le mancate conformità. Mediante un triage sistematico, i CSS danno la priorità agli incidenti identificati concernenti la sicurezza e documentano le informazioni rilevanti necessarie al trattamento di un incidente da parte del servizio competente.</p>		
Contesto		
<p>L'identificazione degli incidenti concernenti la sicurezza nell'ambito di un'organizzazione si effettua generalmente secondo procedure definite e precise che i CSS devono rispettare nello svolgimento dei loro compiti. L'utilizzo di procedure e di strumenti a scopi di sorveglianza dei sistemi deve tener conto delle disposizioni della protezione della personalità e della protezione dei dati.</p> <p>Rapporto con il campo di competenze operative C: il trattamento degli incidenti identificati concernenti la sicurezza è descritto nel campo di competenze operative C.</p> <p>Rapporto con il campo di competenze operative D: l'identificazione di incidenti concernenti la sicurezza può generare nella pratica dei bisogni di soluzioni di sicurezza più estesi o più complessi. Questi bisogni sono generalmente trattati nell'ambito di progetti specifici, al di fuori della gestione operativa normale. Le competenze operative dei CSS legate a progetti sono descritte nel campo di competenze operative D.</p>		
Competenza operativa	Precisazioni sul contenuto e terminologia specifica	Criteri di prestazione (CP)
B1: controllare i sistemi di monitoraggio in funzione	<ul style="list-style-type: none"> <li>- Procedure e strumenti per sorvegliare (monitoring) reti, applicazioni, servizi server, soluzioni di stoccaggio, dispositivi finali e periferici</li> <li>- Soluzioni tecniche (appliances) per individuare attacchi quali Firewall, Intrusion Prevention Systeme (IPS) o Webapplication-Firewalls (WAF)</li> <li>- Security Information and Event Management (SIEM)</li> </ul>	<p>I CSS sono in grado:</p> <p>CP-B-1: di spiegare le strutture, i processi e le interdipendenze nell'ambito dell'organizzazione che sono rilevanti per la loro attività</p> <p>CP-B-2: di spiegare l'organizzazione strutturale e funzionale specifica alla gestione degli incidenti</p> <p>CP-B-3: di selezionare e attuare delle procedure e degli strumenti di sorveglianza dei sistemi</p> <p>CP-B-4: di spiegare le soluzioni tecniche che permettono di identificare degli attacchi e assicurarne il funzionamento</p>
B2: analizzare e interpretare dati	<ul style="list-style-type: none"> <li>- Valutazione automatizzata o manuale delle registrazioni (logfiles)</li> <li>- Rilevamento di falsi positivi</li> <li>- Linguaggi di scripting per la valutazione dei dati</li> <li>- Metodi di analisi dei dati</li> </ul>	

	- Tecniche di rappresentazione allo scopo di sintetizzare le informazioni	CP-B-5: di valutare ed interpretare i vari sistemi in diversi formati
B3: effettuare il triage degli incidenti concernenti la sicurezza	- Rispetto delle direttive e dei processi interni - Classificazione e priorità degli incidenti - Attribuzione (dispatching) degli incidenti	CP-B-6: di programmare, mediante linguaggi di scripting, delle funzioni per la valutazione dei dati
B4: documentare gli incidenti concernenti la sicurezza	- Issue-Tracking-Systeme (ITS) per la gestione degli incidenti lungo tutto il loro ciclo di vita - Elementi informativi su un incidente resp. ticket	CP-B-7: di analizzare e/o paragonare il contenuto degli insiemi di dati nonché di sintetizzare e rappresentare le informazioni ottenute
B5: sorvegliare il trattamento di un incidente concernente la sicurezza	- Operational resp. Service Levels Agreements (OLA, SLA) per il trattamento degli incidenti - Procedure di escalation secondo OLA resp. SLA	CP-B-8: di classificare gli incidenti identificati concernenti la sicurezza, attribuire loro un ordine di priorità e assegnarli ai servizi competenti
<b>Competenze personali e sociali</b>		
	- Capacità di ragionamento e di pensiero sistemico - Disciplina, perseveranza e senso di responsabilità in occasione dell'identificazione di incidenti - Capacità di analisi e pensiero in rete in occasione dell'analisi e della raccolta dei dati - Senso della precisione e buona espressione scritta per la documentazione degli incidenti - Capacità di comunicazione e intelligenza emozionale nell'ambito del lavoro in gruppo e scambi con gli stakeholder	CP-B-9: di utilizzare sistemi di Issue-Tracking e documentare gli incidenti concernenti la sicurezza lungo tutto il loro ciclo di vita CP-B-10: di valutare se le disposizioni OLA o SLA sono rispettate e, se necessario, prevedere procedure di escalation CP-B-11: di valutare la conformità legale e normativa di tutte le misure intraprese nella fase dell'identificazione

### 3.4 CCO C: gestione degli incidenti concernenti la sicurezza

Descrizione del campo di competenze operative (CCO)		
<p>Il CCO C include le competenze operative esercitate dai Cyber Security Specialists (CSS) nel settore <b>Reazione</b>. Le attività che rientrano in questo campo comprendono la gestione degli incidenti concernenti la sicurezza accaduti in fase di attività corrente e il sostegno tecnico fornito durante la gestione di situazioni urgenti o di crisi nell'ambito del Business Continuity Managements (BCM) di un'organizzazione.</p> <p>In caso di incidenti gravi in materia di sicurezza, i CSS implementano misure tecniche immediate allo scopo di ridurre le ripercussioni dirette e i danni di un incidente. In questo contesto, l'acquisizione delle prove rilevanti è la base per l'analisi di un incidente concernente la sicurezza e, se del caso, per le indagini penali e digitali-forensi.</p> <p>I CSS esaminano le cause e le ripercussioni degli incidenti concernenti la sicurezza. Sulla base delle loro analisi e conformemente al piano di reazione agli incidenti dell'organizzazione, i CSS implementano delle misure di protezione reattive o raccomandano misure correttive o preventive alle autorità decisionali. A seguito di una panne del sistema, i CSS sostengono i servizi competenti nel ripristino corretto del funzionamento.</p>		
Contesto		
<p>La gestione degli incidenti concernenti la sicurezza nell'ambito di un'organizzazione avviene generalmente secondo procedure definite e precise che i CSS devono rispettare nello svolgimento dei loro compiti. L'adozione di misure immediate o di protezione deve tener conto delle interdipendenze con le altre unità organizzative e processi (ad es. transizione dei servizi ICT e funzionamento dei servizi, conformità, organizzazione in caso di urgenza e di crisi). È questo il motivo per cui i CSS devono imperativamente disporre di conoscenze approfondite dell'organizzazione strutturale e funzionale della loro impresa o amministrazione.</p> <p>Per quanto concerne la disponibilità e la conservazione delle prove, i metodi e principi applicati per garantire l'utilizzo giuridico dei mezzi di prova devono rispettare le disposizioni legali applicabili nella fattispecie.</p> <p>Rapporto con il campo di competenze operative D: l'analisi delle cause di un incidente concernente la sicurezza può generare nella pratica dei bisogni di soluzioni di sicurezza più estesi o più complessi. Questi bisogni sono generalmente trattati nell'ambito di specifici progetti, al di fuori della gestione corrente. Le competenze operative dei CSS legate a progetti sono descritte nel campo di competenze operative D.</p>		
Competenza operativa	Precisazioni sul contenuto e terminologia specifica	Criteri di prestazione (CP)
C1: attuare misure immediate	<ul style="list-style-type: none"> <li>- Direttive del piano di reazione agli incidenti</li> <li>- Misure tecniche immediate, ad es. isolamento, disattivazione o blocco dei sistemi e servizi</li> </ul>	<p>I CSS sono in grado:</p> <p>CP-C-1: di spiegare le strutture, i processi e le interdipendenze nell'ambito della loro organizzazione che sono rilevanti per la loro attività</p> <p>CP-C-2: di spiegare l'organizzazione strutturale e funzionale specifica alla gestione degli incidenti</p> <p>CP-C-3: di interpretare e applicare le direttive del piano di reazione agli incidenti dell'organizzazione</p>
C2: assicurare la conservazione delle prove	<ul style="list-style-type: none"> <li>- Basi e principi forensi</li> <li>- Conformità legale</li> <li>- Metodi di conservazione delle prove (post mortem, live response)</li> </ul>	
C3: analizzare le cause e le ripercussioni	<ul style="list-style-type: none"> <li>- Analisi degli attacchi</li> <li>- Malware Analyse statica e dinamica</li> </ul>	

	<ul style="list-style-type: none"> <li>- Principi forensi, reti e memorie</li> <li>- Metodi e tecnica di analisi strutturata delle cause</li> </ul>	CP-C-4: di selezionare ed implementare misure tecniche immediate adattate alla situazione e al contesto e di verificare la loro efficienza
C4: definire e attuare misure di protezione	<ul style="list-style-type: none"> <li>- Misure di protezione tecniche e organizzative (MTO)</li> <li>- Interfacce con altri stakeholder e altri processi</li> </ul>	CP-C-5: di assicurare la conservazione delle prove conformemente ai principi che reggono il loro utilizzo legale
C5: sostenere il ripristino dei sistemi	<ul style="list-style-type: none"> <li>- Business Continuity Management (BCM)</li> <li>- Misure di recupero dopo il disastro (desasterrecovery)</li> </ul>	CP-C-6: di analizzare le cause e le ripercussioni degli attacchi mediante metodi e procedure appropriati
<b>Competenze personali e sociali</b>		
<ul style="list-style-type: none"> <li>- Capacità di ragionare nei processi, pensiero sistemico</li> <li>- Facoltà di analisi e pensiero in rete durante l'esame delle cause e delle ripercussioni</li> <li>- Estrema precisione, cura e rigore in occasione dell'identificazione e conservazione dei mezzi di prova e della loro analisi</li> <li>- Confidenzialità e integrità nel trattamento dei mezzi di prova</li> <li>- Creatività e capacità d'innovazione in occasione dello sviluppo di soluzioni</li> <li>- Facilità di comunicazione e intelligenza emotiva nell'ambito del lavoro in gruppo e degli scambi con le parti interessate</li> </ul>		<p>CP-C-7: di spiegare dei metodi e delle procedure di analisi dei Malware</p> <p>CP-C-8: di utilizzare degli strumenti per effettuare delle analisi forensi digitali dei sistemi, reti e memorie</p> <p>CP-C-9: di definire delle misure di protezione reattive appropriate</p> <p>CP-C-10: di formulare e presentare alle autorità decisionali delle raccomandazioni in un linguaggio adeguato ai loro interlocutori</p> <p>CP-C-11: di implementare delle misure di protezione reattive tenendo conto delle parti interessate e di verificare la loro efficienza</p> <p>CP-C-12: di consigliare un'organizzazione di crisi e di urgenza in materia di cybersicurezza con un approccio orientato a bisogni e soluzioni</p> <p>CP-C-13: di valutare la conformità legale e normativa di tutte le misure che rientrano nel campo Reazione</p>

### 3.5 CCO D: pianificazione e attuazione di soluzioni concernenti la sicurezza

Descrizione del campo di competenze operative (CCO)		
<p>Il CCO D include le competenze operative esercitate dai Cyber Security Specialists (CSS) nei settori <b>Business Engineering, Gestione di progetti e Direzione</b>. Queste competenze sono rilevanti quando si tratta di esaminare, sotto forma di progetto, nuovi bisogni o cambiamenti in materia di soluzioni di sicurezza.</p> <p>I CSS specificano, tenendo conto delle parti interessate, delle esigenze funzionali e non funzionali misurabili, che devono essere colmate attraverso soluzioni di sicurezza; in seguito essi analizzano la loro integrazione nel sistema globale nonché le loro interfacce con queste ultime. Se necessario, verificano l'affidabilità e l'efficacia di soluzioni in materia di sicurezza in un contesto specifico.</p> <p>I CSS determinano e inseriscono nel budget, all'attenzione delle autorità decisionali, il personale e i mezzi operativi richiesti dalla soluzione di sicurezza. Sulla base di esigenze definite, procedono alla valutazione delle offerte e delle varianti e sostengono i servizi interessati nell'acquisizione delle soluzioni di sicurezza.</p> <p>Nell'ambito di progetti, i CSS sono responsabili di singoli lavori o sotto-progetti. Essi stabiliscono la pianificazione di progetti, assicurano la comunicazione con tutte le parti interessate in occasione dell'attuazione del progetto, verificano la realizzazione degli obiettivi e adottano, se necessario, misure di coordinamento o misure correttive. In quanto capi di un team di un'unità organizzativa o di responsabili di un sotto-progetto, i CSS possono dirigere dei piccoli gruppi di esperti.</p>		
Contesto		
<p>I progetti nel campo della cybersicurezza vengono elaborati in un contesto di lavoro caratterizzato da problemi complessi, da esigenze interdisciplinari e da cambiamenti frequenti. Oltre a vaste conoscenze specialistiche di diversi campi d'attività e metodi, i CSS devono anche disporre di competenze sociali e personali per poter fronteggiare la complessità dei compiti che incombono loro.</p>		
Competenza operativa	Precisazioni sul contenuto e terminologia specifica	Criteri di prestazione (CP)
D1: delimitare i sistemi e specificare le esigenze	<ul style="list-style-type: none"> <li>- Modellizzazione dei sistemi, dei sotto-sistemi e dei limiti del sistema</li> <li>- Descrizione delle interfacce</li> <li>- Specificazione di esigenze misurabili</li> </ul>	<p>I CSS sono in grado:</p> <p>CP-D-1: di analizzare e di valutare dei sistemi e dei processi</p> <p>CP-D-2: di definire e descrivere le interfacce</p> <p>CP-D-3: di specificare le esigenze dei sistemi in contesti complessi</p> <p>CP-D-4: di verificare e valutare la fattibilità delle soluzioni di sicurezza</p> <p>CP-D-5: di calcolare i costi generati dalle soluzioni di sicurezza</p> <p>CP-D-6: di sviluppare dei criteri di valutazione delle soluzioni di sicurezza</p> <p>CP-D-7: di confrontare e valutare delle varianti</p> <p>CP-D-8: di consigliare i servizi interessati circa le soluzioni di sicurezza e sostenere la loro acquisizione</p>
D2: verificare l'affidabilità e l'efficienza	<ul style="list-style-type: none"> <li>- Metodi di verifica dell'affidabilità (ad es. proof of concept, Feasibility Study, Prototyping, progetti pilota)</li> </ul>	
D3: determinare l'investimento in risorse e inserirlo nel budget	<ul style="list-style-type: none"> <li>- Metodi di stima dei costi</li> <li>- Pianificazione e calcolo dei costi</li> <li>- Controlling di progetti e reporting</li> </ul>	
D4: procedere a una valutazione	<ul style="list-style-type: none"> <li>- Elaborazione di criteri di valutazione</li> <li>- Mansionario e capitolato d'oneri con specificazione delle esigenze</li> <li>- Confronto delle varianti</li> </ul>	

	- Sostegno durante i processi di negoziazione e di acquisizione	CP-D-9: di pianificare dei sotto-progetti a livello di contenuto e risorse
D5: attuare un progetto	- Pianificazione di progetti o di sotto-progetti - Gestione dei rischi e comunicazione - Assicurazione della qualità - Controlling finanziario e reporting	CP-D-10: di sorvegliare dei sotto-progetti e di valutare il loro stato di avanzamento
D6: dirigere un team	- Comportamento manageriale adeguato al contesto e alla situazione - Modelli e regole di comunicazione - Team building e motivazione - Gestione dei conflitti	CP-D-11: di definire e attuare misure di coordinamento e correttive idonee al contesto e alla situazione nell'ambito dei sotto-progetti
<b>Competenze personali e sociali</b>		CP-D-12: di guidare e sviluppare un team sul piano tecnico e sociale
<ul style="list-style-type: none"> <li>- Capacità di comunicazione e orientamento clientela durante il rilevamento dei requisiti</li> <li>- Pensiero sistemico e buona espressione scritta durante la specificazione delle esigenze</li> <li>- Creatività e capacità d'innovazione in occasione dello sviluppo di soluzioni</li> <li>- Capacità di analisi di interdipendenze complesse nell'ambito di progetti interdisciplinari</li> <li>- Senso di responsabilità, coscienza dei costi e della qualità nell'ambito dei progetti</li> <li>- Competenze decisionali nell'ambito dei progetti</li> <li>- Spirito di squadra, facilità di comunicazione e capacità di motivare gli altri nella conduzione di un gruppo</li> <li>- Capacità di gestire dei conflitti e capacità di imporsi nell'ambito della conduzione di un gruppo</li> </ul>		CP-D-13: di gestire in maniera proattiva i conflitti in seno ai gruppi e sviluppare soluzioni costruttive