ICT Berufsbildung
Formation professionnelle
Formazione professionale

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

Mandante	ICT-Formazione professionale Svizzera
Direzione di progetto	eduxept AG
Autori	Stephan Leiser, Jörg Aebischer
Classificazione	nessuna
Status	validato

Modifiche			
Data	Versione	Modifiche	Chi?
25.09.2018	0.1	Versione iniziale sulla base di un workshop	S. Leiser
27.09.2018	0.2	Lettorato e feedback a livello di contenuti	J. Aebischer
12.10.2018	0.3	Adattamenti sulla base dei feedback del comitato di coordinamento e del gruppo di lavoro	S. Leiser
15.10.2018	0.9	Consegna alla SEFRI	ICT-FPCH, J. Aebischer
23.10.2018	1.0	Validazione da parte della SEFRI	SEFRI, S. Ryan
30.10.2018	1.0	Pubblicazione del sito Internet del progetto	ICT-FPCH
27.02.2019	1.1	Numerazione dei criteri di prestazione	S. Leiser

Indice

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 contribuscono 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** →

A	**Protezione preventiva dei sistemi**	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	**Identificazione di incidenti concernenti la sicurezza**	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		
C	**Gestione degli incidenti concernenti la sicurezza**	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		
D	**Pianificazione e attuazione di soluzioni concernenti la sicurezza**	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)		
Il CCO A include le competenze operative esercitate dai Cyber Security Specialist (CSS) nei settori **Anticipazione** e **Prevenzione**. 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. 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. 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. 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.		
Contesto		
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. 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. 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. 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.		
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 CP-A-2: di valutare la credibilità delle fonti e delle informazioni CP-A-3: di ampliare le loro conoscenze sulle minacce in maniera continua, proattiva e autonoma
A2: analizzare le minacce e trattare le informazioni	- Concetto e livelli della Cyber Threat Intelligence (CTI) (strategico, tattica, operativo e tecnico)	
A3: identificare i punti vulnerabili	- Audit e tipi di audit (audit dei sistemi, audit dei processi, audit dell'efficienza e audit della conformità)	

	- Procedure e strumenti per i test di penetrazione, i Vulnerability-Scans e i Compliance-Scans - Indicators of Compromise (IoC) e Indicators of Attack (IoA) - Threathunting proattivo - Quadro legale in materia di pirateria informatica	CP-A-4: di spiegare il concetto di Cyber Threat Intelligence CP-A-5: di identificare la rilevanza delle minacce per la loro organizzazione CP-A-6: di preparare, realizzare e valutare degli audit CP-A-7: di selezionare e utilizzare delle procedure e degli strumenti per identificare i punti vulnerabili in funzione del contesto e dei sistemi CP-A-8: di definire e attuare misure di protezione tecniche od organizzative appropriate CP-A-9: di selezionare ed utilizzare procedure e strumenti appropriati per ingannare gli aggressori CP-A-10: di valutare la conformità legale e normativa di tutte le misure prese nei settori Anticipazione e Prevenzione CP-A-11: di consigliare gli stakeholder sul piano tecnico secondo un approccio orientato ai bisogni e alle soluzioni CP-A-12: di elaborare dei contenuti specializzati in maniera metodologica e didattica CP-A-13: di pianificare, svolgere e valutare delle formazioni
A4: porre rimedio ai punti vulnerabili	- Direttive della strategia di sicurezza dell'informazione (polizia di sicurezza dell'informazione [PSI]) - Misure di protezione tecniche e organizzative (MTO) specifiche ai sistemi, soluzioni di sicurezza e best practice - Metodi di inasprimento dei sistemi (hardening)	
A5: utilizzare procedure ingannevoli	- Procedure e strumenti per ingannare gli aggressori (ad es. Honeypots, Traps, Decoys o strumenti che servono a mascherarsi)	
A6: fornire consulenze tecniche agli Stakeholder	- Principi della consulenza sistemica orientata alle soluzioni - Modelli e regole di comunicazione	
A7: formare gli Stakeholder	- Principi metodologici e didattici - Pianificazione e svolgimento di formazioni	
Competenze personali e sociali		
- Curiosità e disponibilità ad imparare - Capacità di cambiare prospettiva (pensare come un aggressore) - Senso di responsabilità nell'utilizzo di procedure sensibili per individuare i punti vulnerabili o ingannare gli aggressori - Confidenzialità e integrità nel trattamento dei dati e delle informazioni sensibili - Facilità di comunicazione nell'ambito delle attività di consulenza e di formazione		

3.3 CCO B: Identificazione di incidenti concernenti la sicurezza

Descrizione del campo di competenze operative (CCO)		
Il CCO B include le competenze operative esercitate dai Cyber Security Specialists (CSS) nel settore **Identificazione.** Le attività che rientrano in questo campo concorrono all'identificazione degli incidenti concernenti la sicurezza nella gestione operativa. 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.		
Contesto		
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. Rapporto con il campo di competenze operative C: il trattamento degli incidenti identificati concernenti la sicurezza è descritto nel campo di competenze operative C. 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.		
Competenza operativa	**Precisazioni sul contenuto e terminologia specifica**	**Criteri di prestazione (CP)**
B1: controllare i sistemi di monitoraggio in funzione	- Procedure e strumenti per sorvegliare (monitoring) reti, applicazioni, servizi server, soluzioni di stoccaggio, dispositivi finali e periferici - Soluzioni tecniche (appliance) per individuare attacchi quali Firewall, Intrusion Prevention Systeme (IPS) o Webapplication-Firewalls (WAF) - Security Information and Event Management (SIEM)	I CSS sono in grado: CP-B-1: di spiegare le strutture, i processi e le interdipendenze nell'ambito dell'organizzazione che sono rilevanti per la loro attività CP-B-2: di spiegare l'organizzazione strutturale e funzionale specifica alla gestione degli incidenti CP-B-3: di selezionare e attuare delle procedure e degli strumenti di sorveglianza dei sistemi CP-B-4: di spiegare le soluzioni tecniche che permettono di identificare degli attacchi e assicurarne il funzionamento
B2: analizzare e interpretare dati	- Valutazione automatizzata o manuale delle registrazioni (logfiles) - Rilevamento di falsi positivi - Linguaggi di scripting per la valutazione dei dati - Metodi di analisi dei dati	

	- Tecniche di rappresentazione allo scopo di sintetizzare le informazioni	CP-B-5: di valutare ed interpretare i vari sistemi in diversi formati CP-B-6: di programmare, mediante linguaggi di scripting, delle funzioni per la valutazione dei dati CP-B-7: di analizzare e/o paragonare il contenuto degli insiemi di dati nonché di sintetizzare e rappresentare le informazioni ottenute CP-B-8: di classificare gli incidenti identificati concernenti la sicurezza, attribuire loro un ordine di priorità e assegnarli ai servizi competenti 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
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	
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	
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	
Competenze personali e sociali		
- 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		

3.4 CCO C: gestione degli incidenti concernenti la sicurezza

Descrizione del campo di competenze operative (CCO)		
Il CCO C include le competenze operative esercitate dai Cyber Security Specialists (CSS) nel settore **Reazione**. 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. 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. 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.		
Contesto		
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. 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. 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.		
Competenza operativa	**Precisazioni sul contenuto e terminologia specifica**	**Criteri di prestazione (CP)**
C1: attuare misure immediate	- Direttive del piano di reazione agli incidenti - Misure tecniche immediate, ad es. isolamento, disattivazione o blocco dei sistemi e servizi	I CSS sono in grado: CP-C-1: di spiegare le strutture, i processi e le interdipendenze nell'ambito della loro organizzazione che sono rilevanti per la loro attività CP-C-2: di spiegare l'organizzazione strutturale e funzionale specifica alla gestione degli incidenti CP-C-3: di interpretare e applicare le direttive del piano di reazione agli incidenti dell'organizzazione
C2: assicurare la conservazione delle prove	- Basi e principi forensi - Conformità legale - Metodi di conservazione delle prove (post mortem, live response)	
C3: analizzare le cause e le ripercussioni	- Analisi degli attacchi - Malware Analyse statica e dinamica	

	- Principi forensi, reti e memorie - Metodi e tecnica di analisi strutturata delle cause	CP-C-4: di selezionare ed implementare misure tecniche immediate adattate alla situazione e al contesto e di verificare la loro efficienza CP-C-5: di assicurare la conservazione delle prove conformemente ai principi che reggono il loro utilizzo legale CP-C-6: di analizzare le cause e le ripercussioni degli attacchi mediante metodi e procedure appropriati CP-C-7: di spiegare dei metodi e delle procedure di analisi dei Malware CP-C-8: di utilizzare degli strumenti per effettuare delle analisi forensi digitali dei sistemi, reti e memorie CP-C-9: di definire delle misure di protezione reattive appropriate CP-C-10: di formulare e presentare alle autorità decisionali delle raccomandazioni in un linguaggio adeguato ai loro interlocutori CP-C-11: di implementare delle misure di protezione reattive tenendo conto delle parti interessate e di verificare la loro efficienza CP-C-12: di consigliare un'organizzazione di crisi e di urgenza in materia di cybersicurezza con un approccio orientato a bisogni e soluzioni CP-C-13: di valutare la conformità legale e normativa di tutte le misure che rientrano nel campo Reazione
C4: definire e attuare misure di protezione	- Misure di protezione tecniche e organizzative (MTO) - Interfacce con altri stakeholder e altri processi	
C5: sostenere il ripristino dei sistemi	- Business Continuity Management (BCM) - Misure di recupero dopo il disastro (desasterrecovery)	
Competenze personali e sociali		
- Capacità di ragionare nei processi, pensiero sistemico - Facoltà di analisi e pensiero in rete durante l'esame delle cause e delle ripercussioni - Estrema precisione, cura e rigore in occasione dell'identificazione e conservazione dei mezzi di prova e della loro analisi - Confidenzialità e integrità nel trattamento dei mezzi di prova - Creatività e capacità d'innovazione in occasione dello sviluppo di soluzioni - Facilità di comunicazione e intelligenza emotiva nell'ambito del lavoro in gruppo e degli scambi con le parti interessate		

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

Descrizione del campo di competenze operative (CCO)		
Il CCO D include le competenze operative esercitate dai Cyber Security Specialists (CSS) nei settori **Business Engineering, Gestione di progetti** e **Direzione.** Queste competenze sono rilevanti quando si tratta di esaminare, sotto forma di progetto, nuovi bisogni o cambiamenti in materia di soluzioni di sicurezza. 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. 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. 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.		
Contesto		
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.		
Competenza operativa	**Precisazioni sul contenuto e terminologia specifica**	**Criteri di prestazione (CP)**
D1: delimitare i sistemi e specificare le esigenze	- Modellizzazione dei sistemi, dei sotto-sistemi e dei limiti del sistema - Descrizione delle interfacce - Specificazione di esigenze misurabili	I CSS sono in grado: CP-D-1: di analizzare e di valutare dei sistemi e dei processi CP-D-2: di definire e descrivere le interfacce CP-D-3: di specificare le esigenze dei sistemi in contesti complessi CP-D-4: di verificare e valutare la fattibilità delle soluzioni di sicurezza CP-D-5: di calcolare i costi generati dalle soluzioni di sicurezza CP-D-6: di sviluppare dei criteri di valutazione delle soluzioni di sicurezza CP-D-7: di confrontare e valutare delle varianti CP-D-8: di consigliare i servizi interessati circa le soluzioni di sicurezza e sostenere la loro acquisizione
D2: verificare l'affidabilità e l'efficienza	- Metodi di verifica dell'affidabilità (ad es. proof of concept, Feasability Study, Prototyping, progetti pilota)	
D3: determinare l'investimento in risorse e inserirlo nel budget	- Metodi di stima dei costi - Pianificazione e calcolo dei costi - Controlling di progetti e reporting	
D4: procedere a una valutazione	- Elaborazione di criteri di valutazione - Mansionario e capitolato d'oneri con specificazione delle esigenze - Confronto delle varianti	

	- Sostegno durante i processi di negoziazione e di acquisizione	CP-D-9: di pianificare dei sotto-progetti a livello di contenuto e risorse CP-D-10: di sorvegliare dei sotto-progetti e di valutare il loro stato di avanzamento CP-D-11: di definire e attuare misure di coordinamento e correttive idonee al contesto e alla situazione nell'ambito dei sotto-progetti CP-D-12: di guidare e sviluppare un team sul piano tecnico e sociale CP-D-13: di gestire in maniera proattiva i conflitti in seno ai gruppi e sviluppare soluzioni costruttive
D5: attuare un progetto	- Pianificazione di progetti o di sotto-progetti - Gestione dei rischi e comunicazione - Assicurazione della qualità - Controlling finanziario e reporting	
D6: dirigere un team	- Comportamento manageriale adeguato al contesto e alla situazione - Modelli e regole di comunicazione - Team building e motivazione - Gestione dei conflitti	
Competenze personali e sociali		
- Capacità di comunicazione e orientamento clientela durante il rilevamento dei requisiti - Pensiero sistemico e buona espressione scritta durante la specificazione delle esigenze - Creatività e capacità d'innovazione in occasione dello sviluppo di soluzioni - Capacità di analisi di interdipendenze complesse nell'ambito di progetti interdisciplinari - Senso di responsabilità, coscienza dei costi e della qualità nell'ambito dei progetti - Competenze decisionali nell'ambito dei progetti - Spirito di squadra, facilità di comunicazione e capacità di motivare gli altri nella conduzione di un gruppo - Capacità di gestire dei conflitti e capacità di imporsi nell'ambito della conduzione di un gruppo		