EIT.swiss
Limmatstrasse 63
8005 Zürich
044 444 17 17
www.eitswiss.ch

## Identificativo modulo

| | |
|---|---|
| N. modulo | **232** |
| Titolo | **Garantire la sicurezza informatica e la protezione dei dati di un progetto DCM** |
| | |
| Competenze | Identificare le minacce e i punti deboli dei progetti DCM. Assicurare le risorse materiali con le necessarie misure di protezione e secondo lo stato attuale della tecnica. |
| | |
| Obiettivi operativi | 1. Elaborare le misure sulla base delle informazioni raccolte per la sicurezza del sistema di un progetto DCM. |
| | 2. Elaborare le misure di sicurezza e di protezione informatica per soddisfare i requisiti legali e operativi. |
| | 3. Definire le misure di protezione proattive che garantiscono la continuazione delle attività. |
| | |
| Campo di competenza | Security / Risk Management |
| Oggetto | Misure per garantire la sicurezza informatica e la protezione dei dati di un progetto DCM semplice. |
| Attestazione | |
| Anno di tirocinio | 4 |
| Livello | |
| Requisiti | |
| Ore lavoro/lezioni | 40 |
| Riconoscimento | AFC |
| Competenze operative informatici degli edifici AFC | a2: verificare e riportare in un mansionario i requisiti tecnici e quelli relativi alla sicurezza informatica e alla protezione dei dati di un progetto DCM semplice |

ICT Berufsbildung
Formation professionnelle
Formazione professionale

## Competenze operative

Le conoscenze operative necessarie descrivono il sapere che supporta l'esecuzione competente delle attività di un modulo. Queste conoscenze servono da orientamento e non sono definitive. La conseguente concretizzazione degli obiettivi di apprendimento e la determinazione del percorso di apprendimento per l'acquisizione delle competenze sono responsabilità dell'offerente della formazione.

| | | | |
|---|---|---|---|
| N. modulo | | | **232** |
| Titolo | | | **Garantire la sicurezza informatica e la protezione dei dati di un progetto DCM** |
| Campo di competenza | | | Security / Risk Management |
| | | | |
| Obiettivi di valutazione e conoscenze operative | 1 | 1.1 | Conoscono mezzi e metodi semplici per rilevare lacune nella sicurezza e difetti di configurazione nei sistemi (es. Portscanner, Hardening Tools). |
| | | 1.2 | Capiscono il significato di una documentazione completa in relazione alla sicurezza del sistema. |
| | | 1.3 | Conoscono i più comuni errori nella sicurezza della configurazione di sistemi. |
| | | 1.4 | Conoscono il metodo e gli ambiti d'applicazione per raccogliere informazioni sullo stato delle cose in modo mirato e efficiente (es. workshop, analisi dei processi, studio dei documenti). |
| | 2 | 2.1 | Conoscono le fonti dove trovare le descrizioni e le documentazioni relative alle prescrizioni operative e legali (es. descrizioni di funzioni e processi, direttive, organigrammi). |
| | | 2.2 | Conoscono lo stato attuale delle tecniche e delle fonti d'informazione (es. Centro nazionale per la cibersicurezza NCSC), al fine di formulare raccomandazioni sui miglioramenti e sulle possibilità di ampliamento della protezione dei dati e della sicurezza informatica. |
| | | 2.3 | Conoscono diverse misure e i rispettivi vantaggi e svantaggi (es. organizzative, tecniche), che servono a garantire la sicurezza delle informazioni (es. autorizzazioni di accesso, orari di funzionamento, archiviazione dati, protezione password). |
| | 3 | 3.1 | Conoscono le tecniche di applicazione per prevenire l'avaria di processi supportati ICT (es. tolleranze, ridondanze). |
| | | 3.2 | Conoscono misure proattive per minimizzare le conseguenze in caso di avaria di un processo supportato ICT (es. piani d'emergenza, impianto gruppo di continuità). |
| | | | |