



## DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

# CISO (Chief Information Security Officer) – Corso

Prezzo / emissione attestato

**Su richiesta**

IVA/VAT esclusa

Codice corso

**CISO\_LA**

Durata minima

**60 min**

Soglia finale

**70%**

Edizione scheda

**13/10/2026**

## 1. Identità, finalità e perimetro del percorso

Il corso CISO (Chief Information Security Officer) è progettato per formare professionisti in grado di gestire e coordinare la sicurezza informativa nelle organizzazioni, focalizzandosi su best practice internazionali come ISO/IEC 27001, ISO/IEC 27002 e il framework NIST Cybersecurity. Attraverso una combinazione di teoria e casi pratici, i partecipanti approfondiranno le competenze necessarie per valutare e mitigare i rischi, gestire incidenti di sicurezza, e garantire la protezione delle infrastrutture IT e OT/ICS. Il percorso formativo copre aspetti gestione asset, controllo accessi, sicurezza delle reti, applicazioni e risposte agli incidenti, con particolare attenzione a contesti specifici come ospedali, aziende SaaS, gruppi manifatturieri e pubbliche amministrazioni. Al termine, i partecipanti avranno una visione integrata della sicurezza aziendale e gli strumenti per sviluppare piani strategici di sicurezza, supportando il business e la compliance normativa.

La presente scheda tecnica estesa descrive il percorso così come pubblicato nella CIWZ Academy alla data di emissione. Riunisce finalità, riferimenti, architettura didattica, contenuti dei moduli, sistema delle verifiche, criteri di superamento e condizioni di attestazione. Il documento non sostituisce i testi ufficiali delle norme, delle leggi, delle linee guida o degli schemi richiamati.

## 2. Riferimenti normativi, regolamentari e tecnici

ISO/IEC 27001 e ISO/IEC 27002 + ISO/IEC 27005 (risk management) + NIST Cybersecurity Framework (CSF) e best practice di governance della sicurezza delle informazioni

I riferimenti sono utilizzati come quadro di studio e di valutazione nei limiti del contenuto pubblicato e delle fonti disponibili. Per l'applicazione professionale prevalgono sempre le versioni ufficiali e vigenti dei documenti richiamati.

## 3. Architettura didattica e sistema di verifica

- tempo minimo tracciato: 60 min
- banca esame finale attiva: 200 quesiti

- esame finale: 30 quesiti selezionati dalla banca
- soglia di superamento: 70%
- Accesso diretto alla prova finale secondo le regole pubblicate per il percorso “solo test”.
- Composizione dell'esame dalla banca attiva del corso e valutazione secondo la soglia pubblicata.
- Registrazione dell'esito e, quando previsto, richiesta dell'attestato finale.

## 4. Informazioni tecniche ufficiali di catalogo

### Obiettivi formativi

- Formare professionisti in grado di dirigere la sicurezza delle informazioni aziendali
- Approfondire standard normativi e framework come ISO/IEC 27001, 27002, 27005 e NIST CSF
- Sviluppare competenze pratiche in gestione del rischio, sicurezza OT/ICS, network, applicazioni e incident response

### Competenze acquisite

- Valutazione e mitigazione dei rischi cybersecurity
- Gestione della sicurezza in ambienti IT e OT/ICS
- Implementazione di controlli di sicurezza fisica e logica
- Coordinamento di risposte a incidenti di sicurezza

### Destinatari

- Professionisti IT e security manager
- Responsabili compliance e audit
- Consulenti e analisti di sicurezza

### Prerequisiti

- Conoscenze di base di IT e reti
- Familiarità con concetti di sicurezza informatica

### Programma

- Standard ISO/IEC 27001, 27002 e ISO/IEC 27005
- NIST Cybersecurity Framework
- Gestione asset e classificazione informazioni
- Security governance e gestione delle modifiche
- Incident response e threat intelligence
- Controlli operativi per network, applicazioni, IAM
- Case study su contesti ospedalieri, SaaS, manifatturiero, PA

### Metodologia didattica

- Lezioni teoriche
- Analisi di casi reali
- Domande di approfondimento a difficoltà elevata

**Modalità di valutazione**

---

- Test con domande a scelta multipla su scenari pratici
- Passaggio con almeno 70% di risposte corrette

**Durata**

---

- 60 minuti

**Attestazione**

---

- Certificato di frequenza rilasciato a superamento del test con contributo economico

**Risultati attesi**

---

- Capacità di sviluppare e gestire strategie di sicurezza efficaci
- Maggiore consapevolezza dei rischi tecnologici
- Competenze operative per migliorare la security governance

## 7. Sistema di verifica, esame finale e criteri di superamento

- La prova finale è composta da 30 quesiti selezionati dalla banca attiva del corso. La piattaforma applica una logica anti-ripetizione per i nuovi tentativi quando la consistenza della banca lo consente.
- Consistenza della banca finale rilevata al momento della generazione: 200 quesiti attivi.
- Soglia di superamento pubblicata per il corso: 70%.
- Le domande sono finalizzate a verificare non soltanto il richiamo mnemonico, ma anche interpretazione, applicazione, selezione delle evidenze, valutazione di scenari e qualità della decisione, in funzione della materia trattata.

## 8. Tracciamento, continuità didattica e integrità della sessione

- Lo stato del percorso, i moduli completati e il tempo registrato sono gestiti lato server quando il corso utilizza la modalità formativa Academy.
- La piattaforma consente la ripresa del percorso dal punto registrato e conserva gli esiti delle verifiche previste.
- Le sessioni di verifica possono essere soggette ai controlli di integrità e proctoring attivati dalla piattaforma e descritti nelle regole di utilizzo applicabili.
- Gli eventi tecnici e di integrità sono elementi di supporto alla valutazione e non sostituiscono il giudizio professionale quando è prevista una revisione umana.

## 9. Attestazione, utilizzo e limiti del documento

L'attestato CIWZ, quando previsto dal percorso e richiesto dopo il superamento, documenta il risultato ottenuto nel percorso o nella prova CIWZ indicata. Non sostituisce automaticamente certificazioni di persona, iscrizioni ad albi, abilitazioni professionali, qualifiche legali o credenziali rilasciate da organismi o soggetti terzi quando tali requisiti sono previsti dallo schema applicabile.

## 10. Condizioni economiche e fiscali

- Prezzo / emissione attestato: Su richiesta IVA/VAT esclusa.
- La UAE VAT viene applicata ai clienti UAE secondo i dati di fatturazione e la normativa fiscale applicabile.
- Eventuali condizioni commerciali specifiche, convenzioni o ordini aziendali prevalgono sul prezzo pubblico solo se formalmente accettati da Certificato IWZ FZCO.

## 11. Controllo documentale della scheda

- Documento generato automaticamente dalla CIWZ Academy sulla base dei dati del corso pubblicati al momento della richiesta.
- Codice corso: CISO\_LA

- Lingua documento: IT
- Data di generazione: 13/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.