

SCHEDA CORSO INFORMATION SECURITY OFFICER

Dati del corso

Voce	Dettaglio
Titolo	Corso Information Security Officer
Erogato da	Fata Informatica S.r.l. – CybersecurityUP
Tipo	Corso propedeutico alla certificazione CISA/CISO
Modalità	E-learning, con Nomad Learning
Struttura	Corso unico, articolato in 19 aree tematiche
Materiali	Audio lezioni registrate e libro in formato PDF scaricabile
Durata	11 ore
Lingua	Italiano
Accesso	h24, per 12 mesi dalla data di iscrizione
Supporto	Forum per interagire con i docenti
Certificazioni	CISA al superamento dell'esame; CISO in presenza dei requisiti previsti

Presentazione e finalità

Il corso si rivolge ai manager che desiderano avanzare nella propria carriera con una formazione di livello superiore. Attraverso un percorso approfondito, i partecipanti affrontano normativa, pilastri della sicurezza, rischio informatico, progettazione sicura e molto altro, per affinare le competenze indispensabili a eccellere nel ruolo di Chief Information Security Officer, Chief Information Officer, Information Security Officer & Manager, Director of Security & Security Manager, IT Director & Manager.

Il corso offre risorse didattiche progettate per una fruizione agevole e veloce e la possibilità di interazione diretta con il docente attraverso un forum dedicato.

A termine del percorso e con il superamento dell'esame si ottiene la certificazione CISA (Certified Information Security Associate), che attesta il percorso formativo. Il percorso soddisfa inoltre il requisito di formazione necessario per l'accesso all'esame di certificazione CISO (Certified Information Security Officer), fermo restando il rispetto degli ulteriori requisiti previsti dalla normativa vigente.

A chi è rivolto e requisiti per iscriversi

Il corso è progettato per soddisfare le esigenze dei professionisti che mirano a occupare posizioni di leadership nel settore della cybersecurity e nella gestione delle informazioni. Ruoli di riferimento: Chief Information Security Officer, Chief Information Officer, Information Security Officer & Manager, Director of Security & Security Manager, IT Director & Manager.

Requisiti per iscriversi. È necessaria una solida conoscenza della sicurezza informatica, della gestione dei rischi e della protezione dei dati. È utile avere:

- esperienza nella gestione della sicurezza IT;
- familiarità con normative come GDPR e ISO/IEC 27001;
- competenze nella gestione di incidenti di sicurezza;
- abilità di leadership e gestione, perché il corso è orientato alla figura del CISO e alla gestione delle politiche di sicurezza.

Fata Informatica non fornisce consulenza sulle esigenze formative del Cliente: la scelta del corso è responsabilità dell'acquirente.

Obiettivi formativi

Al termine del corso il discente sarà in grado di:

- Descrivere le competenze, le sfide e le tendenze del ruolo del Certified Information Security Officer.
- Orientarsi nel quadro normativo: direttive NIS e NIS2, Agenzia per la Cybersicurezza Nazionale, Perimetro di Sicurezza Cibernetica Nazionale, GDPR.
- Applicare i pilastri della sicurezza (triade CIA, Parkerian Hexad, identità, autenticazione, autorizzazione e responsabilità, non ripudio, due care e due diligence).
- Valutare il rischio informatico partendo da minacce, vulnerabilità e impatto.
- Impostare progettazione sicura, Identity and Access Management e test di sicurezza su sistemi e applicazioni.
- Gestire le security operations: incident management, threat intelligence, continuità operativa, prevenzione e rilevamento.
- Comprendere cloud, nuove architetture (microservizi, container, IoT, edge, fog e grid computing) e crittografia.
- Riconoscere gruppi APT, tecniche d'attacco (Kill Chain, MITRE ATT&CK e D3FEND), malware, botnet e attacchi DDoS.
- Prepararsi all'esame per la certificazione CISA e al percorso verso la certificazione CISO.

Gli argomenti trattati sono dettagliati nel programma.

Struttura del corso

Il corso è unico (non modulare) e propedeutico alla certificazione CISO. Il programma è articolato in 19 aree tematiche, elencate nel programma dettagliato:

Area	Argomento
1	Il Certified Information Security Officer
2	Normativa
3	I pilastri della sicurezza
4	Il rischio informatico
5	La progettazione sicura
6	Identity and Access Management
7	Test di sicurezza su sistemi ed applicazioni
8	Protocolli ed architetture
9	Security operations
10	Cloud e modelli di servizio

Area	Argomento
11	Le nuove architetture
12	La crittografia
13	La rete TOR
14	I gruppi APT
15	Gli attacchi
16	I malware
17	Le botnet
18	Attacchi DDoS
19	Addendum

Al corso si affianca, riservato a chi ottiene la certificazione CISO, il **CISO Elite Club** per l'aggiornamento professionale (vedi sezione Verifiche, attestati e certificazioni).

Modalità di erogazione e metodologia didattica

Il corso è erogato in e-learning, con la metodologia Nomad Learning, ed è pensato per una fruizione agevole e veloce da parte di manager e professionisti.

Elemento	Dettaglio
Nomad Learning	Metodologia di fruizione del corso
Audio lezioni	Registrate, chiare ed efficaci
Accesso	h24, con credenziali personali (username e password)
Libro	In formato PDF scaricabile
Forum di supporto	Per interagire direttamente con i docenti
Esame e certificazione finale	Esame per il conseguimento della certificazione CISA

CISO Elite Club

Lo spazio formativo esclusivo dedicato ai Certified Information Security Officer che hanno ottenuto la certificazione professionale, per un aggiornamento continuo e il mantenimento della certificazione in modo semplice e flessibile. Attraverso questa piattaforma i professionisti ottengono gli 8 crediti CPE annui richiesti dalla normativa.

Il club mette a disposizione documenti ufficiali e studi di settore da fonti autorevoli come NIST, ENISA, ISO, ISACA e altre. Dopo aver consultato il materiale, i membri completano un quiz a scelta multipla: il suo superamento dà automaticamente gli 8 crediti CPE validi per il mantenimento annuale della certificazione.

Verifiche, attestati e certificazioni

Titolo	Chi lo ottiene	Come
CISA – Certified Information Security Associate	Chi completa il corso	Superamento dell'esame finale; attesta il percorso formativo svolto

Titolo	Chi lo ottiene	Come
CISO – Certified Information Security Officer	Chi possiede i requisiti previsti	Esame di certificazione CISO; il corso soddisfa il requisito di formazione

In assenza dei requisiti per la CISO, il percorso formativo consente di sostenere gli esami per la CISA, che attesta le competenze acquisite e rappresenta un primo passo verso la professionalizzazione. Le modalità d'esame sono illustrate durante le lezioni. Il mancato superamento dell'esame non consente di conseguire la certificazione.

Certificazione CISO

La CISO è rilasciata da Fata Informatica, ente accreditato secondo ISO/IEC 17024:2012 e conforme alle norme UNI 11506:2021 e UNI 11621-4:2024. È progettata per esperti di sicurezza informatica che ricoprono ruoli di leadership e gestione nelle organizzazioni, e attesta competenze avanzate nella definizione di politiche di sicurezza, nella gestione dei rischi informatici e nella leadership dei team di sicurezza. In linea con la Legge 4/2013, i professionisti certificati saranno inseriti nel registro Accredia dei Certified Information Security Officer.

Requisiti per la CISO

- Istruzione: almeno il diploma di scuola secondaria di primo grado.
- Formazione: almeno 8 ore di aggiornamento nell'ultimo anno.
- Esercizio dell'attività di CISO: 2 anni per chi possiede una laurea o corsi di formazione tecnica superiore dopo la scuola superiore, 3 anni per chi ha completato la scuola superiore, 4 anni per chi possiede il diploma di scuola media.

Mantenimento. Ogni anno il professionista trasmette a Fata Informatica l'evidenza di formazione continua specifica nell'ambito CISO (corsi, convegni o sfide su piattaforme), l'evidenza di continuità professionale (o di incremento della formazione, in caso di perdita di lavoro) e l'evidenza della registrazione e del trattamento di eventuali reclami ricevuti. Gli 8 crediti CPE annui si ottengono con il CISO Elite Club.

Rinnovo. Al quinto anno il professionista presenta l'assenza o la corretta gestione dei reclami, il continuo esercizio della professione, i crediti formativi acquisiti negli anni di mantenimento, supera l'esame di rinnovo e paga la relativa quota, come indicato nel tariffario ufficiale. In funzione degli esiti il certificato può essere rinnovato, sospeso o revocato.

Le certificazioni sono progettate per formare esperti del settore e differiscono per contenuti, metodologia d'esame, conformità normativa e valore nel mercato europeo.

Programma dettagliato

Il corso comprende audio lezioni registrate, accesso h24, libro in PDF scaricabile, forum di supporto con i docenti ed esame finale. Il programma è articolato nelle 19 aree tematiche seguenti.

1. **Il Certified Information Security Officer.** Le competenze · Sfide e tendenze.
2. **Normativa.** La direttiva NIS · La direttiva NIS2 · L'Agenzia per la Cybersicurezza Nazionale · Il Perimetro di Sicurezza Cibernetica Nazionale · La General Data Protection Regulation.
3. **I pilastri della sicurezza.** La triade CIA · Il Parkerian Hexad · Divulgazione, Alterazione e Distruzione · Identità, Autenticazione, Autorizzazione e Responsabilità · Non repudiazione · Limitazioni dei privilegi e necessità di sapere · Due care e Due diligence.
4. **Il rischio informatico.** Minacce, vulnerabilità e impatto · Il rischio.
5. **La progettazione sicura.** Pratiche di progettazione sicura · Modelli di sicurezza.
6. **Identity and Access Management.** I metodi di autenticazione · Tecnologie di controllo accessi · Modelli di autorizzazione · I sistemi di gestione degli accessi · Protocolli di autenticazione e autorizzazione.

- 7. Test di sicurezza su sistemi ed applicazioni.** Security Assessment · Il processo di security code review · Misurare la sicurezza.
- 8. Protocolli ed architetture.** Architettura di rete · Lo stack TCP/IP · Le applicazioni web.
- 9. Security operations.** La sicurezza amministrativa · Incident Management · La Threat intelligence · La continuità operativa · Prevenzione e rilevamento · La sicurezza nella posta elettronica.
- 10. Cloud e modelli di servizio.** La responsabilità condivisa nell'era del cloud computing.
- 11. Le nuove architetture.** Microservizi · I container · IoT · Edge, Fog e Cloud computing · Il Grid computing.
- 12. La crittografia.** Crittografia a chiave simmetrica · Crittografia asimmetrica · Lo scambio sicuro di chiavi · Hash · Firme crittografiche · Sfide future.
- 13. La rete TOR.** La rete TOR · Navigare in incognito · I servizi nascosti · Attacchi a TOR · Sforzi per rendere TOR sicuro.
- 14. I gruppi APT.** La minaccia APT · Gli obiettivi degli attacchi APT · Gruppi statali vs gruppi criminali · Convenzioni di denominazione.
- 15. Gli attacchi.** La Kill Chain Lockheed Martin · Unified Kill Chain di Paul Pols · MITRE ATT&CK · MITRE D3FEND.
- 16. I malware.** La classificazione dei malware · Le tecniche di evasione · I Ransomware.
- 17. Le botnet.** I componenti principali di una botnet · Architettura del C&C · Utilizzo delle botnet · I meccanismi di protezione · Takedown.
- 18. Attacchi DDoS.** Tipologia di attacchi · Mitigazione · Evoluzione degli attacchi DDoS.
- 19. Addendum.** I documenti nello sviluppo e deploy del software · Termini e Condizioni nei contratti di acquisto · L'outsourcing · I processi di innovazione.

Requisiti hardware e software

Per accedere al corso il Cliente deve disporre dei requisiti seguenti. La verifica è a carico del Cliente (Condizioni di Vendita, art. 4 e art. 11).

Componente	Requisito
Personal computer	Per le sessioni di teoria e pratica sono necessari PC desktop o notebook, mentre per la fruizione dei contenuti teorici è possibile utilizzare dispositivi mobile. In particolare nelle sessioni pratiche è suggerito l'uso di PC con processori 64 bit, almeno quad-core, con supporto Intel VT-x / AMD-V o tecnologia equivalente per compatibilità con ambienti di virtualizzazione locali, con minimo 8 GB di RAM (consigliati almeno 16 GB) e almeno 80 GB di spazio libero su disco per l'installazione e l'esecuzione delle macchine virtuali. Monitor con risoluzione minima consigliata di 1280 × 720 pixel. Scheda audio e cuffie o altoparlanti. Webcam e microfono qualora siano previste attività formative in modalità blended.

Componente	Requisito
Software di virtualizzazione	La postazione dedicata alle sessioni pratiche dovrà consentire l'installazione e l'utilizzo di un software di virtualizzazione compatibile con le macchine virtuali messe a disposizione per le esercitazioni, o comunque suggerite nell'ambito dei laboratori quale strumento per la costruzione di un proprio insieme di strumenti. Le VM saranno distribuite in formato OVA. Per la realizzazione di VM al fine della costruzione di un proprio laboratorio è consigliato seguire l'esempio d'uso di ciascun corso al fine di rendere speculare l'esperienza nelle videolezioni con la pratica. In ambito aziendale/corporate è del tutto evidente che l'utente dovrà disporre dei permessi necessari per installare, configurare ed eseguire software e macchine virtuali sulla propria postazione o avere soddisfatti in modo alternativo i requisiti. Per garantire la piena fruibilità delle attività formative e dei laboratori, <u>è pertanto raccomandato l'utilizzo di un PC personale</u> sul quale l'utente disponga di privilegi amministrativi.
Browser	È necessario utilizzare una versione aggiornata e supportata di uno dei principali browser web, quali: • Google Chrome • Mozilla Firefox • Microsoft Edge • Apple Safari Il browser dovrà consentire l'esecuzione di JavaScript, l'utilizzo dei cookie, il download di file e la riproduzione di contenuti multimediali.
Connettività	Connessione Internet ad alta velocità e stabile, necessaria per lo streaming dei video e per accesso ai laboratori

Componente	Requisito
Requisiti di rete e sicurezza	La postazione e la connessione utilizzate devono consentire l'accesso ai servizi Internet necessari alla fruizione della piattaforma e allo svolgimento delle esercitazioni. Eventuali firewall, proxy, VPN, sistemi di filtraggio, DNS filtering, endpoint security o altre policy di sicurezza applicate da reti aziendali/corporate non devono impedire o limitare: • L'accesso alla piattaforma di erogazione e agli eventuali servizi esterni integrati; • Il download dei materiali didattici e delle immagini delle macchine virtuali • La riproduzione di contenuti audio/video • L'utilizzo di cookie, JavaScript e degli altri servizi web richiesti • Eventuali connessioni necessarie allo svolgimento dei laboratori pratici (VPN via UDP in porta non standard) Qualora venga utilizzata una postazione o una rete aziendale soggetta a restrizioni, l'utente dovrà verificare preventivamente la disponibilità dei permessi di installazione, virtualizzazione e accesso alla rete necessari. Per garantire la piena fruibilità delle attività formative e dei laboratori, <u>è pertanto raccomandato l'utilizzo di un PC personale</u> sul quale l'utente disponga di una connessione Internet non soggetta a restrizioni corporate incompatibili con le attività previste.
Lettura documenti	Software di lettura di file in formato .pdf
Audio e video	Software e dispositivi per la riproduzione di file audio e video (casse o cuffie)
Laboratori	I laboratori potranno essere fruibili attraverso: • Materiale scaricabile da sottoporre a strumenti locali (la cui installazione è a carico dell'utente), quali simulatori, analizzatori, ecc. Questi strumenti potranno essere collocati su proprio PC o in apposita VM sperimentale • Connessione Web diretta a piattaforma di simulazione/esercitazione • Connessione VPN (tramite differenti porte) ad infrastrutture virtuali remote. Gli strumenti di indagine devono essere predisposti dall'utente nel proprio PC o all'interno di VM predisposte all'esercitazione. In alcun caso viene fornito un ambiente di analisi o strumentazione di attacco attraverso le piattaforme. ATTENZIONE! In alcuni casi è possibile che il laboratorio trattino materiale pericoloso quale exploit o malware. È fondamentale trattare questi casi in VM isolate e protette in modo da evitare contaminazioni o incidenti alle infrastrutture estranee ai laboratori.

Il Cliente si impegna ad adeguare i propri sistemi hardware e software in caso di aggiornamenti o mutamenti della piattaforma. Fata Informatica non risponde dei difetti di fruizione dovuti al mancato possesso dei requisiti minimi di sistema.

Durata dell'iscrizione, accesso e assistenza

Voce	Dettaglio
Validità dell'iscrizione	12 mesi dalla data di iscrizione
Scadenza	Terminato il periodo, l'iscrizione viene disattivata automaticamente: lezioni e test vanno completati entro la scadenza
Accesso ai materiali	h24, con username e password personali, non cedibili
Area personale	Elenco dei corsi frequentati e dei materiali correlati
Credenziali	Generate automaticamente e inviate dal tutor didattico dopo l'iscrizione e il pagamento
Assistenza didattica	Forum di supporto per interagire con i docenti; sistema di ticket per domande ai docenti e allo staff, attivo per tutta la durata dell'iscrizione, e-mail di supporto supportodidattico@fatainformatica.it
Reclami	Per iscritto a Fata Informatica, Via Tiburtina 912, 00156 Roma; esito comunicato entro 20 giorni lavorativi
CISO Elite Club	Riservato a chi ha ottenuto la certificazione CISO; 8 crediti CPE annui con quiz a scelta multipla

Il Cliente deve svolgere personalmente le lezioni e i test. Eventuali ulteriori informazioni aggiornate sono comunicate dalla parte tecnica il primo giorno di lezione.

Prezzi e modalità di pagamento

I prezzi sono espressi in euro, IVA inclusa. Ogni opzione è acquistabile in un'unica soluzione oppure, dove indicato, a rate. Il pagamento avviene online tramite il servizio Stripe. Fata Informatica non gestisce né memorizza i dati degli strumenti di pagamento. Eseguito il pagamento, viene emessa la fattura. Il pagamento a rate è disponibile solo ove espressamente indicato. Completata l'iscrizione e saldato il prezzo, il Cliente riceve le credenziali di accesso. Il pagamento a rate comporta una maggiorazione del 5%.

Recesso e condizioni di vendita

L'acquisto è regolato dalle Condizioni di Vendita dell'e-commerce di Fata Informatica S.r.l (Rev. 03 del 07.10.2026) che il Cliente accetta con modalità point and click prima dell'acquisto. Il Cliente dichiara di aver letto questa Scheda del Corso prima di acquistare.

- **Recesso (consumatori).** 14 giorni dalla data di acquisto, senza motivazione e senza costi (art. 52 Codice del Consumo).
- **Perdita del recesso.** Il diritto non è più esercitabile dopo l'invio delle credenziali che danno accesso immediato alla piattaforma. Chi vuole recedere deve attendere i 14 giorni prima di ricevere le credenziali.
- **Fruizione immediata.** Il Cliente può chiedere, durante l'ordine, di accedere subito al corso, accettando di perdere il diritto di recesso (art. 59, comma 1, lett. o). Riceve conferma del contratto e ricevuta via e-mail.
- **Rimborso.** In caso di recesso valido, entro 60 giorni dall'esercizio, con riaccredito sullo stesso strumento di pagamento.

- **Diritto d'autore.** Audio lezioni, libro e materiali sono di proprietà di Fata Informatica: è vietato copiarli, distribuirli o cederli. Le credenziali sono personali e non cedibili.
- Il testo completo delle Condizioni di Vendita prevale su quanto qui sintetizzato.