

**SCHEDE REQUISITI**  
**PER LA QUALIFICAZIONE DEI CORSI PER**  
**“CONSULENTI DI SISTEMI DI GESTIONE DELLA**  
**SECURITY ”**

3	18.12.2012	Rev. Generale	<i>Presidente Comitato di Certificazione</i>	<i>Presidente Consiglio Direttivo</i>
2	12.12.2000	Rev. Generale	<i>Presidente Comitato di Certificazione</i>	<i>Presidente Consiglio Direttivo</i>
<b>Rev.</b>	<b>Data</b>	<b>Motivazioni</b>	<b>Convalida</b>	<b>Approvazione</b>

**REQUISITI ORGANIZZATIVI DELL'ENTE EROGANTE IL CORSO**

<b>Organizzazione</b>	L'organizzazione deve designare un proprio rappresentante legale e un responsabile “tecnico” per la didattica (quest'ultimo sarà l'interfaccia CEPAS, per tutti gli aspetti concernenti il processo di qualificazione e di mantenimento).
<b>Risorse umane</b>	L'organizzazione deve utilizzare un team di almeno 3 docenti. Per la docenza devono essere utilizzati: <ol style="list-style-type: none"><li>1) Security Manager o Consulenti della Security, certificati da un Organismo di Certificazione del Personale</li><li>2) Docenti Universitari con esperienza di almeno 10 anni nel settore della security aziendale.</li></ol>
<b>Infrastruttura</b>	L'organizzazione dovrà garantire in ogni edizione del corso l'idoneità dei locali destinati alla formazione, in accordo alla Normativa cogente in vigore, relativamente agli strumenti di supporto didattici (strumenti informatici, audiovisivi ecc.).
<b>Comunicazione</b>	<p>Il corso deve essere presentato ai partecipanti mediante adeguato documento (<i>brochure o altro simile</i>) contenente almeno le seguenti informazioni:</p> <ul style="list-style-type: none"><li>• organizzazione titolare del corso, identificata dal proprio logo (eventuali partner commerciali di supporto devono essere indicati come tali)</li><li>• numero di iscrizione nel Registro CEPAS (a qualificazione ottenuta)</li><li>• luogo e periodo di svolgimento</li><li>• programma didattico dettagliato, struttura e durata in ore del corso (non inferiore ai requisiti minimi CEPAS)</li><li>• scopo e finalità</li><li>• nome del coordinatore tecnico e altri riferimenti della segreteria dell'Organizzazione titolare</li><li>• requisiti di accesso per i partecipanti</li><li>• rilascio dell'attestato di Corso qualificato ai soli partecipanti in possesso dei requisiti di accesso</li><li>• validità del corso come uno dei requisiti per la certificazione CEPAS</li><li>• i percorsi di certificazione CEPAS nel settore Security</li><li>• il numero massimo dei partecipanti (in ogni caso non superiore a 20 persone)</li><li>• assenza consentita (in ogni caso non superiore al 5% sul totale di 120 ore)</li></ul> <p>Su tale documento, il riferimento al possesso della qualificazione CEPAS sarà autorizzato solo a qualificazione ottenuta. In iter di qualificazione può essere apposto solo il riferimento “corso in fase di qualificazione da parte del CEPAS”, previa approvazione CEPAS.</p>

**REQUISITI MINIMI PER IL CORSO**

<b>Durata</b>	120 ore totali di lezioni, esercitazioni ed esami, frazionabili in moduli della durata di almeno 2 giorni consecutivi.
<b>Requisiti di accesso dei partecipanti al corso</b>	<ul style="list-style-type: none"><li>▪ Diploma di Scuola Media Superiore</li><li>▪ Appropriata esperienza di lavoro (4 anni per i diplomati di scuola media superiore e 2 anni per i gradi di istruzione superiore) in attività attinenti la security presso aziende, enti o nella consulenza.</li><li>• Questionario tecnico di ingresso con almeno 15 domande a risposta chiusa (sono esclusi i quesiti con risposte Vero/Falso), relative alla conoscenza di base dei temi del corso</li></ul>
<b>Obiettivi</b>	<ul style="list-style-type: none"><li>▪ conoscenza e comprensione degli argomenti proposti nel corso;</li><li>▪ acquisizione di conoscenze, abilità e caratteristiche personali richieste per l'attività di consulente della security aziendale</li></ul>

**STRUTTURA**

<b>ARGOMENTI</b>	<p><b>Le norme/linee guida citate si intendono nella loro versione vigente/applicabile</b></p> <p><b>MODULO I: Lo scenario di riferimento, la valutazione e la presa in carico dei rischi (durata 26 ore)</b></p> <ul style="list-style-type: none"><li>• normativa nazionale cogente e volontaria: D.Lgs. 231/01, D.Lgs. 196/03, D.M.269/2010, UNI 10459, UNI 10891, ISO 9001, ISO 27001 e ISO 19011</li><li>• evoluzione dei rischi: dal rischio fisico al rischio strategico</li><li>• la strutturazione della funzione di security e le sue interrelazioni interne ed esterne</li><li>• la collocazione organizzativa, la missione e il ruolo della funzione di security</li><li>• l'intelligence preliminare: analisi del territorio, analisi di azienda, analisi del contesto competitivo, analisi dei fenomeni</li><li>• Corporate Security Policy</li><li>• risorse aziendali e risorse critiche</li><li>• l'analisi dei rischi: individuazione e valutazione</li><li>• l'analisi delle vulnerabilità</li><li>• le tipologie di rischi in un approccio integrato di tutela aziendale</li><li>• l'assunzione ed il trasferimento del rischio</li><li>• valutazione dei rischi e politica d'intervento: analisi costi/benefici</li><li>• le tecnologie a supporto dell'Homeland security</li><li>• Esercitazione scritta sugli argomenti</li></ul>
------------------	--

**MODULO II: La risposta organizzativa ai rischi di security  
(durata 30 ore)**

- l'Impresa e i Sistemi di Gestione integrati (Qualità, Ambiente, Safety, ISMS, SA8000)
- la Norma ISO 9001 e la sua evoluzione: le prospettive per la certificazione della Security
- il sistema di gestione della security aziendale secondo ISO 9004 e ISO 10006
- scelte strategiche e pianificazione aziendale della Security
- il modello di pianificazione: esempi specifici
- la Security e la normativa del lavoro (Dlgs 81/08)
- La responsabilità dell'impresa ed il D.Lgs. 231/01
- la Security nei contratti esterni
- la formalizzazione e la diffusione delle procedure di Security
- l'organizzazione della sicurezza pubblica e privata
- la Security e la sicurezza privata: la selezione, l'utilizzo e la gestione dei servizi di sorveglianza in ottemperanza alla L.101/2008 ed al D.M. 1/12/10
- la sicurezza del “top management”.
- piano della progettazione del sistema e assegnazione delle responsabilità
- la gestione delle risorse e la gestione del processo di Security
- verifica, analisi e miglioramento del sistema di gestione della Security
- certificazione della sicurezza e standard di sicurezza:
  - ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems – Requirements
  - ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management
  - ITSEC:1990 - Information Technology Security Evaluation Criteria
  - TCSEC : 1985 - Trusted Computer System Evaluation Criteria
  - ISO/IEC 15408-1:2009 - Information technology - Security techniques - Evaluation criteria for IT security (ex Common Criteria for Information Technology Security Evaluation
  - ISO 22301:2012 - Business Continuity Management Systems (BCSMS)
- Esercitazione scritta sugli argomenti

**MODULO III: Sicurezza delle informazioni  
(durata 26 ore)**

- La tutela delle informazioni aziendali – Riservatezza, Integrità e Disponibilità del patrimonio informativo
- misure di sicurezza del Dlgs 196/03 “sulla privacy”
- reati informatici: aspetti legali in ambito nazionale e internazionale
- sicurezza dei sistemi d'elaborazione isolati: tipologie di attacco, tecniche di difesa HW e SW
- crittografia e firma elettronica
- la sicurezza dei sistemi di telecomunicazioni
- la sicurezza dei sistemi di reti pubbliche di comunicazione
- la sicurezza nel cloud computing
- la sicurezza delle basi di dati: autorizzazioni, piani di backup, procedure di disaster recovery e business continuity, meccanismi di tracing e di auditing

- la sicurezza dei sistemi distribuiti: controllo dell'accesso, profili utente, tecniche di tracing e di auditing, firewall e intrusion detection, per l'interconnessione con la rete Internet, ecc..
- Sicurezza “MOBILE”
- La tutela dei sistemi di trasmissione dati (Wireless, VoIP, fibre ottiche, satellite, Internet)
- Integrazione della RETE WI-FI con i sistemi aziendali di sicurezza
- Sicurezza dei siti internet
- Esercitazione scritta sugli argomenti

**MODULO IV: La risposta operativa ai rischi di Security**  
**(durata 30 ore)**

- Gli strumenti della security aziendale: investigazioni, intelligence, Business Security, etica d'impresa
- l'attuazione del sistema di gestione della security: contenuti/ raccomandazioni/ responsabilità nella realizzazione delle azioni/ pianificazione/ revisione e aggiornamento periodico
- la valutazione costi/benefici e la valutazione della performance del servizio di security
- il budget della security: costi operativi/ costi di loss prevention/ costi di *loss mitigation*
- convalida delle procedure operative
- Le nuove tecnologie di sicurezza fisica ed elettronica: barriere elettroniche, controllo accessi, videosorveglianza, sistemi biometrici, scanner, badge, chiavi elettroniche, smart cards, trasponder, RFID, ecc.
- il “*crisis management*” ed il piano di emergenza
- D.Lgs 231/01 – “Responsabilità amministrativa delle società e modelli di organizzazione, gestione e controllo”, in rapporto alla security aziendale
- I processi di Business Ethics come strumenti di riduzione del rischio
- l'auditing nel sistema di gestione della security (ISO 19011)
- Backup dei dati, Disaster Recovery e Business Continuity
- L'outsourcing delle funzioni di security
- l'intelligence aziendale e la *business intelligence*
- le relazioni istituzionali
- Esercitazione scritta sugli argomenti

<b>Esercitazioni</b>	<p>Le esercitazioni devono costituire il 30% del tempo totale del corso e devono essere svolte, in presenza, nell’ambito degli argomenti sopra elencati e per ciascun modulo.</p> <p>Tutte le esercitazioni devono essere raccolte, registrate e documentate in modo appropriato dall’Organizzazione e devono essere finalizzate alla verifica della conformità ai requisiti fissati per gli argomenti del corso.</p>
<b>Documentazione</b>	<p>Il corso di formazione deve essere definito da un “pacchetto formativo” scritto, documentale e/o multimediale, composto almeno da:</p> <ul style="list-style-type: none"><li>• Questionario tecnico di ingresso con almeno 15 domande a risposta chiusa (sono esclusi i quesiti con risposte Vero/Falso), relative alla conoscenza di base dei temi del corso</li><li>• Guida per il docente che deve contenere:<ul style="list-style-type: none"><li>- descrizione dettagliata dei contenuti</li><li>- descrizione delle esercitazioni da effettuare e utilizzo dei relativi strumenti</li><li>- descrizione delle metodologie didattiche da applicare in ciascuna attività</li><li>- tempi da dedicare a ciascuna attività</li><li>- criteri per la raccolta ed archiviazione delle registrazioni.</li></ul></li><li>• Materiale per il partecipante che deve contenere:<ul style="list-style-type: none"><li>- materiale didattico completo utilizzato in aula</li><li>- una sintesi, in forma descrittiva oppure schematica, di tutti gli argomenti trattati</li><li>- curricula dei singoli docenti</li><li>- una bibliografia selettiva</li><li>- modulo per la valutazione del corso e dei docenti</li><li>- regolamento del corso comprendente i reclami</li><li>- criteri di valutazione delle esercitazioni e delle prove d’esame.</li></ul></li><li>• Guida per la conduzione degli esami finali che deve contenere:<ul style="list-style-type: none"><li>- descrizione per titoli delle prove (scritte e orali) con tempi relativi</li><li>- almeno un esempio (non svolto) di prova scritta</li><li>- almeno 10 esempi di domande per esami orali</li></ul></li></ul> <p>Il pacchetto formativo deve essere firmato dal Progettista del Corso e/o da un Esperto di argomento. Le due persone possono coincidere, se la persona possiede i requisiti di entrambe le funzioni.</p>
<b>Valutazione finale</b>	<p>La valutazione complessiva di ogni partecipante deve essere formalizzata e registrata e deve consentire di determinare se gli obiettivi del corso sono stati conseguiti. La valutazione finale, della durata di 8 ore complessive, deve essere superata con una soglia minima, secondi criteri prestabiliti dall’Organizzazione ed approvati da CEPAS.</p> <p>Devono almeno essere previste una prova scritta, individuale, volta ad accertare le conoscenze acquisite dai candidati e una prova orale applicativa individuale (min. 30 minuti). Alla valutazione finale sono ammessi i soli partecipanti, in possesso di tutti requisiti di accesso al Corso, che, ad esito positivo, riceveranno un attestato di Corso qualificato CEPAS. L’esame di fine corso deve essere sempre condotto da almeno due Docenti. Tutte le singole prove devono essere raccolte e documentate in modo appropriato dall’Organizzazione.</p>

**CONDIZIONI PER IL MANTENIMENTO DELLA QUALIFICAZIONE CEPAS**

<b>Durata della Qualificazione</b>	La qualificazione del corso ha una durata annuale e si rinnova tacitamente di anno in anno, in assenza di revoca e/o rinuncia.
<b>Sorveglianza</b>	Il corso qualificato sarà oggetto di sorveglianza annuale, attraverso verifica diretta (in fase di erogazione del corso) e indiretta (di tipo documentale), nelle sessioni scelte a discrezione da CEPAS.
<b>Prescrizioni (estratto del Protocollo di Accordo MD15)</b>	<p>Tutte le seguenti prescrizioni dovranno essere rispettate dall'Ente erogante il corso</p> <ul style="list-style-type: none"><li>- rispettare i requisiti di cui alla “Scheda/e di riferimento per il corso</li><li>- non cedere, modificare e/o trasferire ad alcun titolo, la qualificazione del corso, senza la preventiva autorizzazione di CEPAS, che se ne riserva l'accettazione previa opportuna verifica e valutazione insindacabili.</li><li>- comunicare entro il 15 gennaio di ogni anno il programma annuale delle edizioni del corso e confermare, 5 giorni prima dell'inizio, ciascuna edizione del corso ed i nominativi dei docenti;</li><li>- consentire ai Commissari incaricati da CEPAS la valutazione periodica (visita di sorveglianza) sia sul campo sia presso la sede dove vengono conservate le registrazioni inerenti la gestione del corso qualificato (es. registrazioni dei reclami o dei requisiti dei partecipanti, monitoraggio dei docenti, risoluzione di non conformità riscontrate);</li><li>- consentire ai Commissari e/o al Personale CEPAS debitamente autorizzato, la valutazione documentale relativa a tutte le edizioni del corso successive all'ottenimento della qualificazione;</li><li>- notificare al CEPAS ogni variazione nei contenuti del programma didattico del corso e/o dei docenti, rispetto a quelli oggetto di qualificazione;</li><li>- inviare a CEPAS, in formato elettronico, entro 15 giorni dal termine del corso, l'elenco dei candidati che hanno superato le singole edizioni, completo di indirizzi, recapiti telefonici/fax, e-mail, autorizzati dai candidati stessi;</li><li>- mantenere un registro dei reclami e dei moduli di valutazione del corso e dei docenti (compilati dai partecipanti al corso stesso) e renderli disponibili, su richiesta, a CEPAS; entro 10 giorni dalla ricezione del reclamo, inviare comunicazione scritta e copia del reclamo stesso a CEPAS</li><li>- versare, alle scadenze previste, le quote annuali relative al mantenimento della qualificazione del corso, indicate nel tariffario CEPAS in vigore;</li><li>- non utilizzare la qualificazione del corso come sinonimo di qualificazione professionale dei partecipanti;</li><li>- non effettuare attività concorrenziale nei confronti di CEPAS.</li></ul>