

**SCHEDA REQUISITI  
PER LA QUALIFICAZIONE DEL  
CORSO PER  
“PROFESSIONISTA DELLA SECURITY AZIENDALE”**

3	08.02.2018	Rev. Generale	<i>Presidente CSI /Schema</i>	<i>Amministratore Delegato</i>
2	28.09.2016	Pag. 1	<i>Presidente Comitato di Schema</i>	<i>Amministratore Delegato</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>	<p>Il corso di formazione di 120 ore deve essere erogato da Università riconosciute dal Ministero dell'Istruzione, dell'Università e della Ricerca oppure da Enti di formazione accreditati presso le Regioni (<i>come indicato nel Prospetto B1 Appendice B della Norma UNI 10459</i>).</p> <p>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).</p>
<b>Risorse umane</b>	<p>L'organizzazione deve utilizzare un team di almeno 3 docenti.</p> <p style="text-align: center;"><b>REQUISITI PER I DOCENTI</b></p> <p>Per la docenza devono essere utilizzati:</p> <ol style="list-style-type: none"><li>1) Senior Security Manager certificati CEPAS</li><li>2) Docenti con esperienza di almeno 10 anni nel settore della security aziendale.</li></ol> <p>Potranno essere previste testimonianze e approfondimenti tematici, da parte di esperti, a supporto degli argomenti sviluppati dai docenti.</p> <p>Potranno anche essere utilizzati assistenti in possesso di diploma di laurea di I livello, con almeno 4 anni di esperienza nell'ambito della formazione e/o della ricerca universitaria o privata, in uno o più argomenti previsti dagli argomenti del corso per security manager. (I loro interventi non dovranno essere complessivamente superiori al 20% dell'intero corso).</p>
<b>Infrastruttura</b>	<p>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.). Per i corsi erogati in modalità FAD dovrà essere garantita la disponibilità di idonea piattaforma dimensionata per l'utenza.</p>
<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>

<b>CEPAS srl</b>	<b>SCHEDA REQUISITI PER LA QUALIFICAZIONE DEL CORSO PER “PROFESSIONISTA DELLA SECURITY AZIENDALE”</b>	<b>Sigla:</b> SH41 <b>Rev.:</b> 3 <b>Pag.:</b> 3 di 7
------------------	---	---

**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 istruzione secondaria superiore</li> <li>▪ Esperienza lavorativa maturata nel settore della security di 2 anni (facoltativo)</li> <li>• Superamento di un 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, con una soglia minima di 10 risposte esatte.</li> </ul>
<b>Obiettivi</b>	<ul style="list-style-type: none"> <li>▪ Conoscenza e comprensione degli argomenti proposti nel corso;</li> <li>▪ Acquisizione delle conoscenze dei compiti del Professionista della Security, con riferimento alla norma UNI 10459:2017, consentendogli di acquisire le conoscenze necessarie e sviluppare le abilità richieste per il conseguimento della certificazione (Security Expert, Security Manager, Senior Security Manager), rilevando, ove possibile, gli aspetti comportamentali legati all’attività di Professionista della Security aziendale, proporzionalmente al grado richiesto.</li> </ul>

**STRUTTURA**

<b>ARGOMENTI</b>	<p><i>Gli argomenti devono essere strutturati secondo quanto indicato nella norma UNI 10459:2017, con riferimento a:</i></p> <ul style="list-style-type: none"> <li>• <i>Appendice A.1: Compiti del Security Expert;</i></li> <li>• <i>Appendice-A.2: Compiti del Security Manager;</i></li> <li>• <i>Appendice A.3: Compiti del Senior Security Manager;</i></li> <li>• <i>Appendice A.4: Conoscenze</i></li> <li>• <i>Appendice A.5: Abilità</i></li> <li>• <i>appendice B: Requisiti per l'accesso ai livelli professionali del professionista della security;</i></li> <li>• <i>appendice C: Aspetti etici e deontologici;</i></li> <li>• <i>appendice D: Aspetti comportamentali</i></li> </ul> <p><b>Conoscenze</b> (rif. Appendice A.4)</p> <p><b>Analisi scenari e contesto</b></p> <ul style="list-style-type: none"> <li>• Analisi scenari di riferimento (geopolitici, sociali, economici, ambientali, tecnologici)</li> <li>• Analisi settore di appartenenza</li> <li>• Analisi organizzativa interna (Struttura organizzativa, Processi critici e operativi, Risorse e aree critiche, Vision, mission, strategia aziendale, Policy, linee guida e procedure aziendali, Codice di condotta, Valore e azienda (economico, mercato e sociale),Principi di sostenibilità, responsabilità sociale, tutela dei diritti umani ed etica</li> </ul> <p><b>Criminologia applicata</b></p> <ul style="list-style-type: none"> <li>• Criminologia applicata e profiling criminale</li> <li>• Criminalità e sicurezza nei contesti urbani (CPTED)</li> </ul>
------------------	---

**ARGOMENTI****Legislazione**

- Sicurezza nella costituzione e sicurezza pubblica (ruoli e responsabilità)
- Responsabilità giuridiche (penali, civili e amministrative) e aziendali
- Elementi di diritto penale
- Responsabilità amministrativa degli enti
- Sicurezza sul lavoro
- Sicurezza privata
- Elementi di sicurezza delle informazioni
- Codice la tutela della proprietà Industriale
- Tutela del know-how e del segreto industriale
- Statuto dei Lavoratori
- Elementi di protezione dei dati personali

**Gestione del rischio (enterprise risk management)**

- Rischi nelle organizzazioni
- Metodologie di analisi
- Politiche di gestione
- Struttura di riferimento per la gestione dei rischi e normativa correlata
- Strumenti di trasferimento a terzi (es. strumenti tecnici e assicurativi)

**Security management**

- Definizione
- Evoluzione storica
- Compiti e attività
- Organizzazione e Relazioni interne ed esterne della security
- Chi e Cosa proteggere: persone, risorse materiali, risorse immateriali, strutture, infrastrutture e infrastrutture critiche, siti e obiettivi sensibili, processi
- Focus su: Sicurezza di luoghi ad alta frequentazione, Sicurezza di porti e aeroporti,
- Sicurezza di eventi e grandi eventi

**Il sistema di gestione dei rischi per la security (security risk management)****Progetto**

- Analisi contesto esterno
- Analisi contesto interno
- Individuazione minacce
- Valutazione rischi
- Selezione politiche di gestione del rischio
- Elaborazione Piano di Security
- Analisi economica e finanziaria degli Investimenti
- Scelta delle soluzioni e attuazione
- Monitoraggio e reporting

**Sistema di gestione**

- Il sistema di gestione della security: applicazioni nei diversi settori e organizzazioni (industriale, telecomunicazioni, trasporto, energia, bancario e finanziario, ecc,...)
- I sistemi di gestione e gli standard di riferimento: qualità, ambiente, sicurezza sul lavoro, sicurezza delle informazioni, sicurezza della catena di fornitura (supply chain), continuità operativa.

**Intelligence e security intelligence**

- Definizioni
- Metodologie e tecniche
- Ambiti di utilizzo
- Attività investigative e indagini in azienda

<b>ARGOMENTI</b>	<p><b>Strumenti di sicurezza</b></p> <ul style="list-style-type: none"><li>• Tecnologie e sistemi di sicurezza passiva</li><li>• Tecnologie e sistemi di sicurezza attiva</li><li>• Strumenti organizzativi di security (policy, procedure, organizzazione, ecc...)</li></ul> <p><b>Servizi di sicurezza e altri servizi</b></p> <ul style="list-style-type: none"><li>• Servizi di sicurezza privata</li><li>• Vigilanza privata: servizi, contratti e normativa di riferimento</li><li>• Investigazione privata: servizi, contratti e normativa di riferimento</li><li>• Servizi di guardiania (portierato, accoglienza, ecc.)</li></ul> <p><b>Sicurezza delle informazioni e delle risorse intangibili (intangible e information security)</b></p> <ul style="list-style-type: none"><li>• Elementi della sicurezza delle informazioni e delle risorse intangibili (marchi, know-how,...)</li><li>• Principali rischi e attacchi al sistema informatico</li><li>• Reati informatici</li><li>• Caratteristiche generali del sistema di gestione per la sicurezza delle informazioni</li><li>• Principali contromisure tecnologiche e organizzative per la sicurezza delle informazioni</li></ul> <p><b>Continuità operativa e gestione delle emergenze (business continuity &amp; emergency management)</b></p> <ul style="list-style-type: none"><li>• Business Continuity e Disaster Recovery: definizione, metodologia e normativa di riferimento</li><li>• Emergency Management: definizione, metodologia, attori coinvolti, comportamento individuale e delle masse, elementi di psicologia delle emergenze, comunicazione in caso di crisi</li></ul> <p><b>Elementi di management</b></p> <ul style="list-style-type: none"><li>• Elementi di strategia, pianificazione e controllo aziendale</li><li>• Elementi di organizzazione del lavoro e gestione delle risorse</li><li>• Elementi di budgeting e finanza aziendale (es. strumenti di valutazione degli investimenti)</li><li>• Elementi di leadership</li><li>• Elementi di project management</li><li>• Elementi di time management</li><li>• Elementi di comunicazione e negoziazione</li></ul> <p>Elementi di gestione dei conflitti, dello stress e del sé nei momenti critici</p>
<b>Esercitazioni</b>	<p>Le esercitazioni devono costituire il 50% del tempo totale del corso e devono essere sviluppate nell'ambito degli argomenti sopra elencati.</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:</p> <ul style="list-style-type: none"><li>- 1 prova scritta, individuale, volta ad accertare le conoscenze acquisite dai candidati</li><li>- 1 prova orale applicativa individuale (min. 30 minuti)</li></ul> <p>Alla valutazione finale sono ammessi i soli partecipanti, in possesso dei requisiti di accesso al Corso, che, ad esito positivo, riceveranno un attestato di Corso qualificato CEPAS.</p> <p>L’esame di fine corso deve essere condotto da 2 Docenti.</p> <p>Tutte le singole prove devono essere raccolte e documentate in modo appropriato dall’Organizzazione.</p> <p>La valutazione del candidato dovrà rispettare i parametri EQF (European Qualifications Framework) indicati nei prospetti su referenziati.</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</b> <i>(estratto del Protocollo di Accordo MD15)</i>	<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 e inviare a CEPAS ogni variazione nei contenuti del programma didattico del corso e/o dei docenti e ogni comunicazione relativa al Corso qualificato (locandina, articoli, pubblicità a mezzo stampa, web) al fine di verificare la coerenza e correttezza delle informazioni rispetto al significato della qualificazione CEPAS;</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 certificazione professionale dei partecipanti</li><li>• non effettuare attività concorrenziale nei confronti di CEPAS</li><li>• utilizzare il fac-simile allegato al Protocollo di Accordo, per l’emissione degli attestati di superamento corso ai partecipanti.</li></ul>